PheeNet

Network Access Control

User's Manual
Version 3.12

WMS-208

Table of Contents

Chapter 1. Before You Start **1**

1.1 Audience 1

1.2 Document Convention 1

Chapter 2. System Overview **2**

2.1 Introduction of WMS-208 2

2.2 System Concept 2

2.3 Capacity and Performance 3

Chapter 3. Base Installation **4**

3.1 Hardware Installation 4

3.1.1 System Requirements 4

3.1.2 Package Contents 4

3.1.3 Panel Function Descriptions 5

3.1.4 Installation Steps 6

3.2 Quick Software Configuration 7

Chapter 4. Web Interface Configuration **17**

4.1 System Configuration 18

4.1.1 Configuration Wizard 19

4.1.2 System Information 20

4.1.3 WAN1 Configuration 22

4.1.4 WAN2 Configuration 24

4.1.5 WAN Traffic Settings 26

4.1.6 LAN Port Mapping 28

4.1.7 Service Zones 31

4.2 User Authentication 37

4.2.1 Authentication Configuration 38

4.2.1.1 Authentication Method - Local 40

4.2.1.2 Authentication Method - POP3 45

4.2.1.3 Authentication Method - RADIUS 46

4.2.1.4 Authentication Method - LDAP 49

4.2.1.5 Authentication Method - NT Domain 51

4.2.1.6 Authentication Method - ONDEMAND 52

4.2.1.7 Authentication Method - SIP 64

4.2.2 Black List Configuration 65

4.2.3 Group Configuration 67

4.2.4 Policy Configuration 71

4.2.5 Additional Configuration 78

4.3 AP Management 81

4.3.1 AP List 82
4.3.2 AP Discovery 87
4.3.3 Manual Configuration 91
4.3.4 Template Settings 92
4.3.5 Firmware Management 93
4.3.6 AP Upgrade 94
4.3.7 WDS Management 95
4.4 Network Configuration 96
4.4.1 Network Address Translation 97
4.4.2 Privilege List 99
4.4.3 Monitor IP List 101
4.4.4 Walled Garden List 102
4.4.5 Proxy Server Properties 103
4.4.6 Dynamic DNS 104
4.4.7 IP Mobility 105
4.4.8 VPN Configuration 106
4.5 Utilities 110
4.5.1 Change Password 111
4.5.2 Backup/Restore Setting 112
4.5.3 Firmware Upgrade 113
4.5.4 Restart 114
4.5.5 Network Utilities 115
4.6 Status 116
4.6.1 System Status 117
4.6.2 Interface Status 119
4.6.3 Routing Table 121
4.6.4 Current Users 123
4.6.5 Traffic History 124
4.6.6 Notification Configuration 127
4.7 Help 129
Appendix A. Accepting Payment via Authorize.Net **130**
Appendix B. Accepting Payment via PayPal **139**
Appendix C. Service Zone Deployment Example **149**
Appendix D. Proxy Setting **161**
Appendix E. Session Limit and Session Log **167**
Appendix F. Network Configuration on PC & User Login **169**
Appendix G. Console Interface **184**
Appendix H. Local VPN **187**
Appendix I. Customizable Pages **192**

Chapter 1. Before You Start

1.1 Audience

This manual is intended for the system or network administrators with the networking knowledge to complete the step by step instructions of this manual in order to use the WMS-208 for a better management of network system and user data.

1.2 Document Convention

- For any caution or warning that requires special attention of readers, a highlight box with the eye-catching italic font is used as below:

Warning: *For security purposes, you should immediately change the Administrator's password.*

Indicate that clicking this button will return to the homepage of this section.

Indicate that clicking this button will return to the previous page.

Indicate that clicking this button will apply all of your settings.

Indicate that clicking this button will clear what you set before these settings are applied.

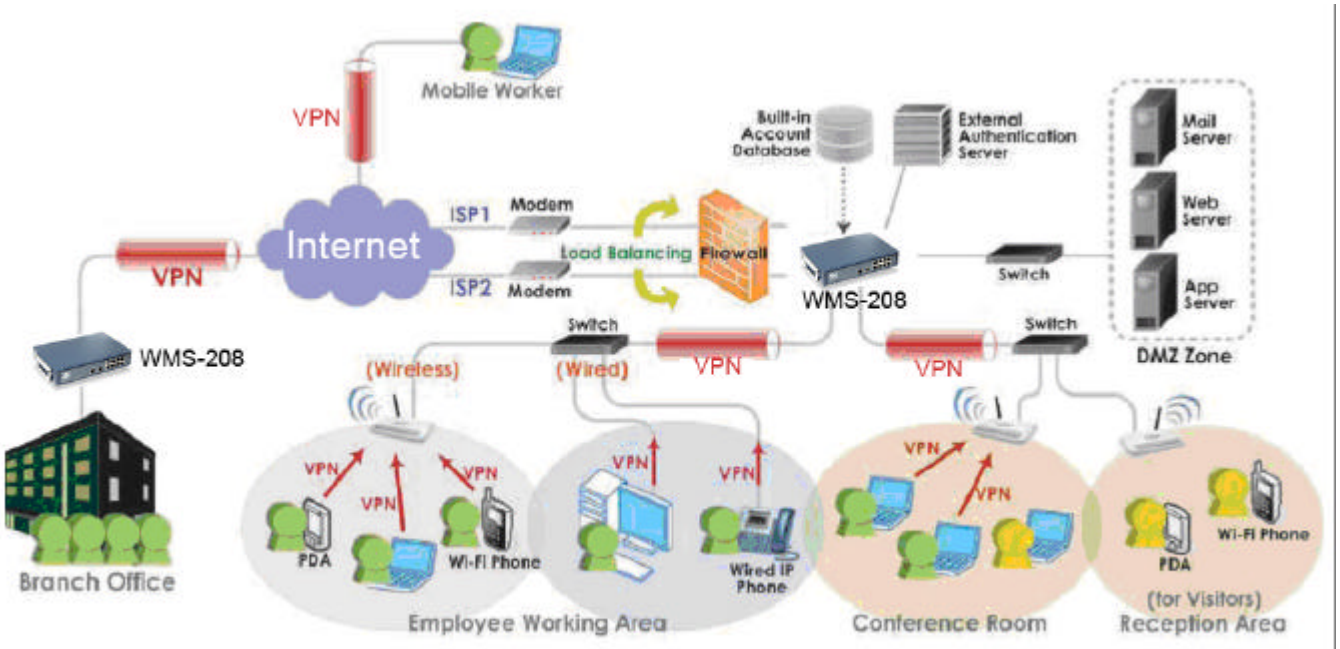
Chapter 2. System Overview

2.1 Introduction of WMS-208

WMS-208 is a Network Access Controller, specially designed for wired and wireless data network environments in small to middle scaled businesses and hotspots. It features integrated management, secured data transmission, and enhanced accounting and billing. System administrators can effectively monitor wired or wireless users, including employees and guest users via its user management interface. Moreover, administrators can discover, configure, monitor, and upgrade all managed Access Points (APs) from a single, centralized AP management interface.

2.2 System Concept

WMS-208 is capable of managing user authentication, authorization and accounting. The user account information is stored in the local database or a specified external database server. Featured with user authentication and integrated with external payment gateway, WMS-208 allows users to easily pay the fee and enjoy the Internet service using credit cards through Authorize.net or PayPal. With centralized AP management feature, the administrator does not need to worry about how to manage multiple wireless access point devices. Furthermore, WMS-208 introduces the concept of Service Zones - multiple virtual networks, each with its own definable network policy. This is very useful for hotspot owners seeking to provide different customers or staff with different levels of network services. The following diagram is an example of WMS-208 set to manage the Internet and network access services at a hotspot venue.



An example of typical SMB network deployment

2.3 Capacity and Performance

Capacity and Performance	***PheeNet WMS-208***
Concurrent Users	120
Local Accounts	1000
On-demand user Accounts	2,000
Managed Access Points (WAP-654G, WAP-854GP)	12
Monitored 3rd-Party Access Points	40
VPN Termination Tunnels	120
VPN 3DES/DES Throughput	30 Mbps

Chapter 3. Base Installation

3.1 Hardware Installation

3.1.1 System Requirements

- Standard 10/100BaseT network cables with RJ-45 connectors
- All PCs need to install the TCP/IP network protocol

3.1.2 Package Contents

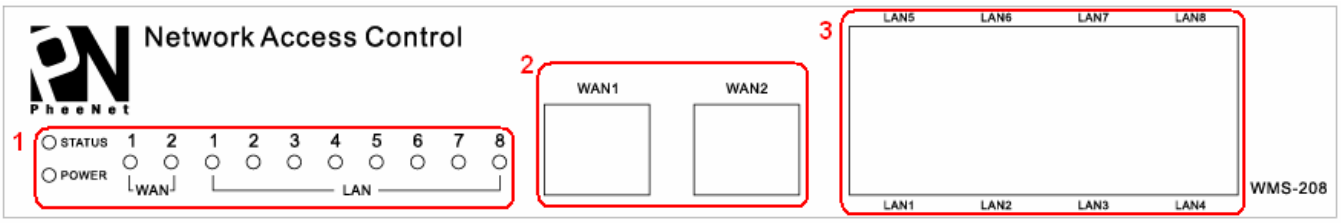
The standard package of PheeNet WMS-208 includes:

- PheeNet WMS-208 x 1
- CD-ROM (with User's Manual and QIG) x 1
- Quick Installation Guide x 1
- DC 12V Power Adapter x 1
- Ethernet Cable x 1
- Console Cable x 1

Warning: *It is highly recommended to use all the supplies in the package instead of substituting any components by other suppliers to guarantee best performance.*

3.1.3 Panel Function Descriptions

Front Panel



? **LED:** There are four kinds of LED, **Power**, **Status**, **WAN** and **LAN**, to indicate different status of the system.
  - **Power:** LED ON indicates power on.
  - **Status:** While system power is on, status OFF indicates BIOS is running; BLINKING indicates the OS is running, and ON indicates system is ready.
  - **WAN:** LED ON indicates connection to the WAN port.
  - **LAN:** LED ON indicates connection to the LAN port.

? **WAN1/WAN2:** Two WAN ports (10 Base-T / 100Base-TX RJ-45) are available on the system.

? **LAN1~LAN8:** Client machines connect to WMS-208 via LAN ports (10 Base-T / 100Base-TX RJ-45).

> ***Note:*** *By Default, all LAN ports are set with Port-based Default Service Zone; for Service Zone configuration, please refer to section 4.1.7.*

Rear Panel

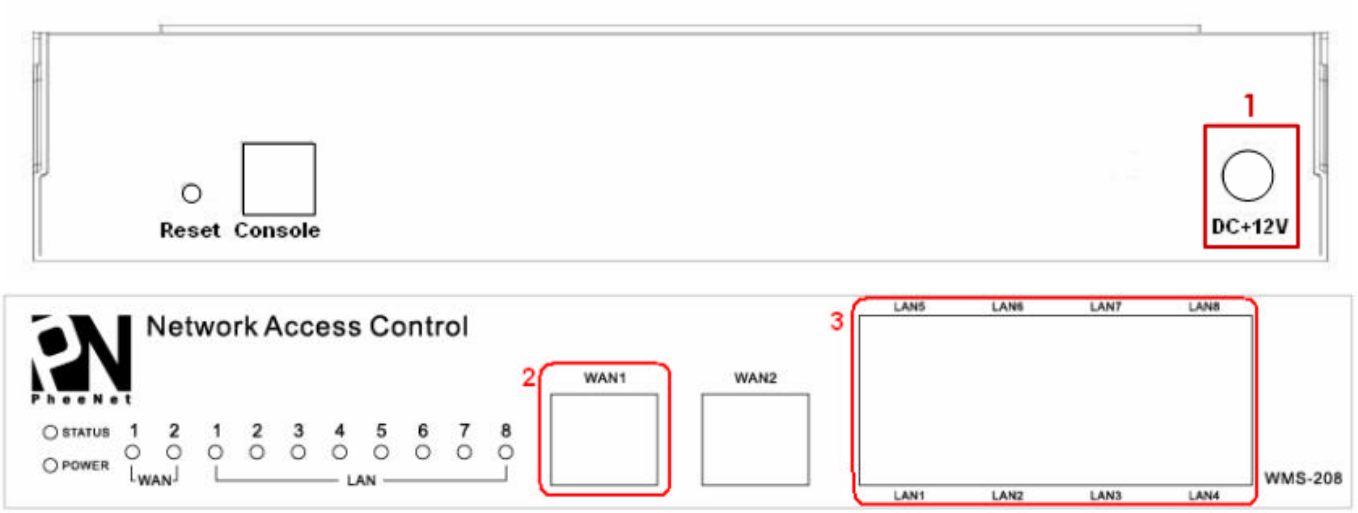
? **Reset:** Press this button to restart the system.

? **Console:** The system can be configured via a serial console port. The administrator can use a terminal emulation program such as Microsoft's HyperTerminal to login to the configuration console interface to change admin password or monitor system status, etc.

? **DC+12V:** The power adapter attaches here.

3.1.4 Installation Steps

Please follow the following steps to install PheeNet WMS-208:



1. Connect the power adapter to the power socket on the rear panel. The Power LED should be on to indicate a proper connection.

2. Connect an Ethernet cable to the WAN1 Port on the front panel. Connect the other end of the cable to an external networking device such as an ADSL modem, a cable modem, a switch, or a hub.

3. Connect an Ethernet cable to one of the LAN1~LAN8 Ports on the front panel. Connect the other end of the Ethernet cable to an administrator's PC or a client PC, AP, or switch in managed network. The LED of the connected port should be on to indicate a proper connection.

Attention:

PheeNet WMS-208 supports Auto Sensing MDI/MDIX. You may use either straight through or cross-over cable to connect the Ethernet Port.

3.2 Quick Software Configuration

PheeNet WMS-208 supports web-based configuration. Upon the completion of hardware installation, WMS-208 can be configured via web browsers with JavaScript enabled such as Internet Explorer version 6.0 and above or Firefox. There are two ways to configure the PheeNet WMS-208 system: using the online **Configuration Wizard** or changing the settings by commands manually. The **Configuration Wizard** comprises of six basic steps as follows. Follow the instructions of Configuration Wizard to enter the required information step by step, save your settings, and restart WMS-208. The 6 steps of Configuration Wizard are listed below:

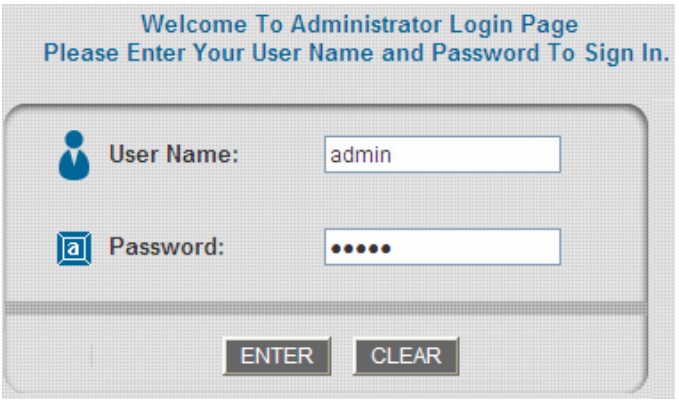
Step 1. Change Admin's Password
Step 2. Choose System' s Time Zone
Step 3. Set System Information
Step 4. Select Connection Type for WAN Port
Step 5. Add Local User Account (Optional)
Step 6. Save and Restart PheeNet WMS-208

Please follow the following steps to complete the quick configuration:

1. To access the web management interface, connect a PC to one of the LAN1~8 ports, and then launch a browse. **Make sure you have set DHCP in TCP/IP of your PC to get an IP address dynamically.**

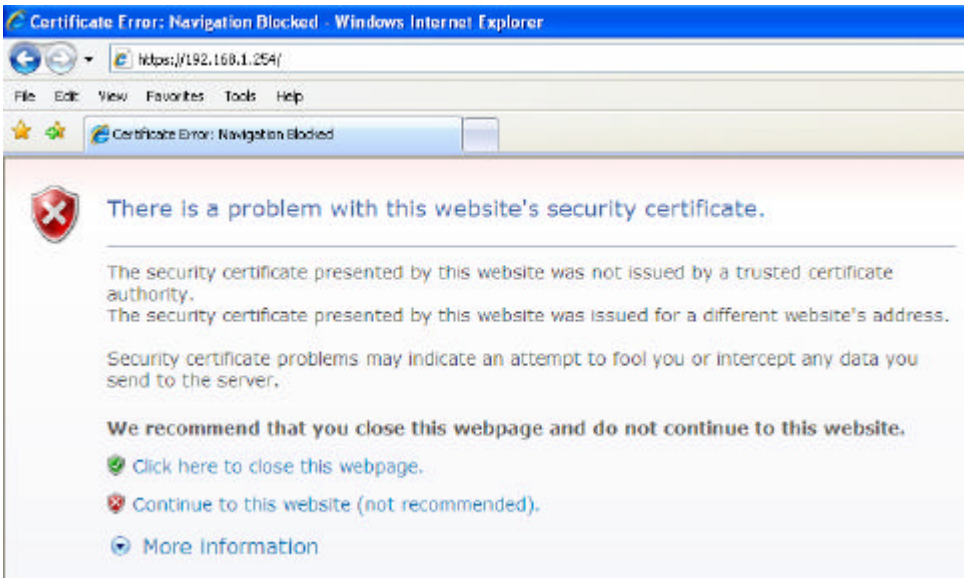
   Next, enter the gateway IP address of WMS-208 at the address field. The default gateway IP address is ***"https://192.168.1.254"*** (**"https"** is used for a secured connection).

   The administrator login page will appear. Enter ***"admin"***, the default username, and ***"admin"***, the default password, in the User Name and Password fields. Click ***Enter*** to log in.



After a successful login, a "Welcome to System Administration" page will appear on the screen.

For the first time, if the WMS-208 is not using a **trusted SSL certificate** (for more information, please see 4.2.5 Additional Configuration), there will be a **"Certificate Error"**, because the browser treats WMS-208 as an illegal website. Please press **"Continue to this website"** to continue. The default user login page will then appear in the browser.


Certificate Error: Navigation Blocked - Windows Internet Explorer
https://192.168.1.254/
File Edit View Favorites Tools Help
Certificate Error: Navigation Blocked
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

Caution: *If you can't get the login screen, the reasons may be:*

(1) The PC is set incorrectly so that the PC can't obtain the IP address automatically from the LAN port;

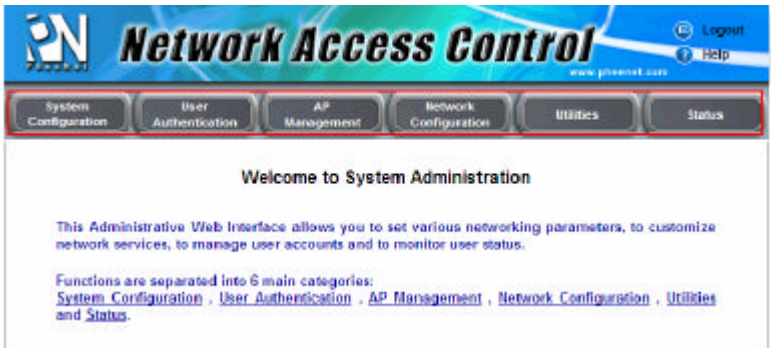
(2) The IP address and the default gateway are not under the same network segment. Please use default IP address such as 192.168.1.xx in your network and then try it again. For the configuration on PC, please refer to ***Appendix F.***

PheeNet WMS-208 supports three kinds of account interface. You can log in as **admin**, **manager** or **operator**. The default username and password as follows.

Admin: The administrator can access all area of the PheeNet WMS-208.

User Name: **admin**

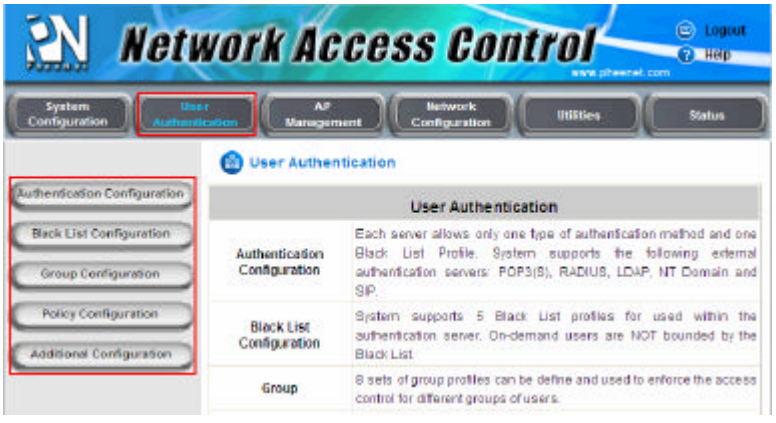
Password: **admin**


Network Access Control
Logout
Help
System Configuration
User Authentication
AP Management
Network Configuration
Utilities
Status
Welcome to System Administration
This Administrative Web Interface allows you to set various networking parameters, to customize network services, to manage user accounts and to monitor user status.
Functions are separated into 6 main categories:
System Configuration , User Authentication , AP Management , Network Configuration , Utilities and Status.

Manager: The manager can access the area under ***User Authentication*** to manage the user account, but no permission to change the settings of the profiles of Firewall, Specific Route and Schedule.

User Name: **manager**

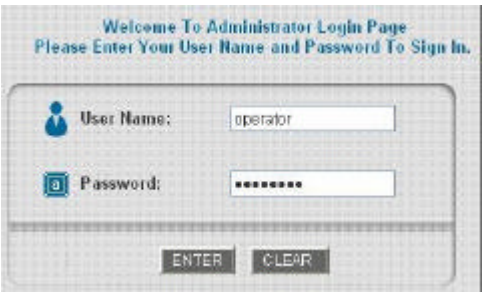
Password: **manager**


Network Access Control
Logout
Help
System Configuration
User Authentication
AP Management
Network Configuration
Utilities
Status
Authentication Configuration
Black List Configuration
Group Configuration
Policy Configuration
Additional Configuration
User Authentication
User Authentication
Authentication Configuration
Each server allows only one type of authentication method and one Black List Profile. System supports the following external authentication servers: POP3(S), RADIUS, LDAP, NT Domain and SIP.
Black List Configuration
System supports 5 Black List profiles for used within the authentication server. On-demand users are NOT bounded by the Black List.
Group
8 sets of group profiles can be define and used to enforce the access control for different groups of users.

Operator: The operator can only access the area of ***Create On-demand User*** to create and print out the new on-demand user accounts.

User Name: **operator**

Password: **operator**



After a successful login to WMS-208, a web management interface with a welcome message will appear.

Note: *To logout, simply click the Logout icon on the upper right corner of the interface to return to the login screen.*

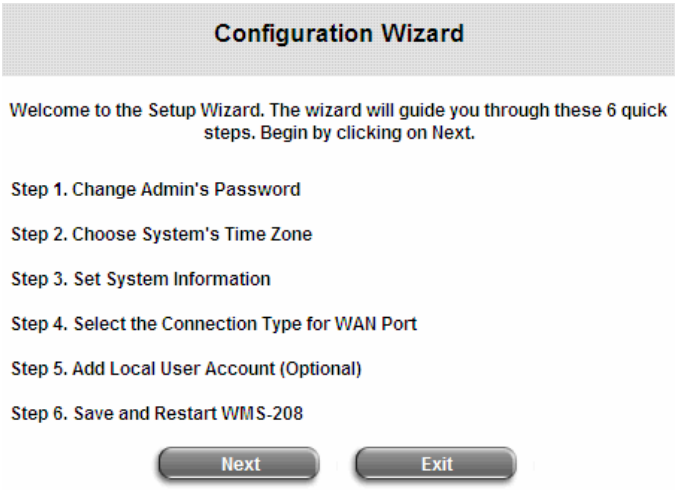
2. Now you are ready to run the Wizard.

To quickly configure WMS-208 by using the **Configuration Wizard**, click ***System Configuration*** from the top menu to go to the **System Configuration** page. Then, click ***Configuration Wizard*** on the left.

Click the ***Run Wizard*** button to begin the **Configuration Wizard**. The **Configuration Wizard** will appear in a pop-up browser window. Click ***Next*** to begin.

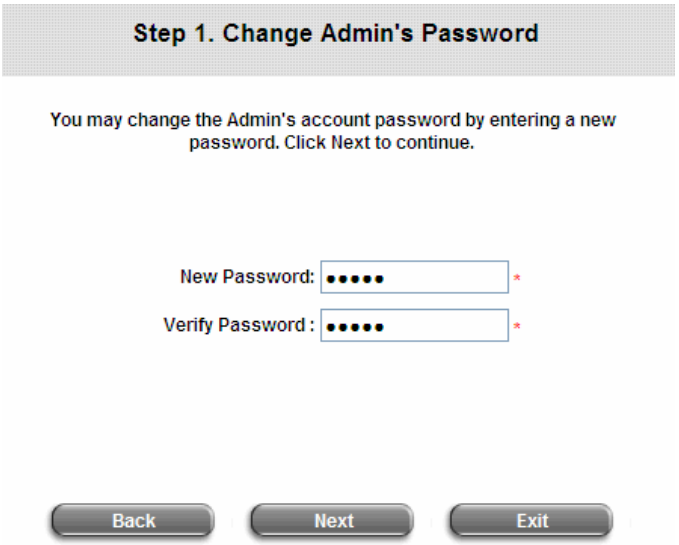
3. Running Configuration Wizard

A welcome screen that briefly introduces the 6 steps will appear. Click ***Next*** to begin.

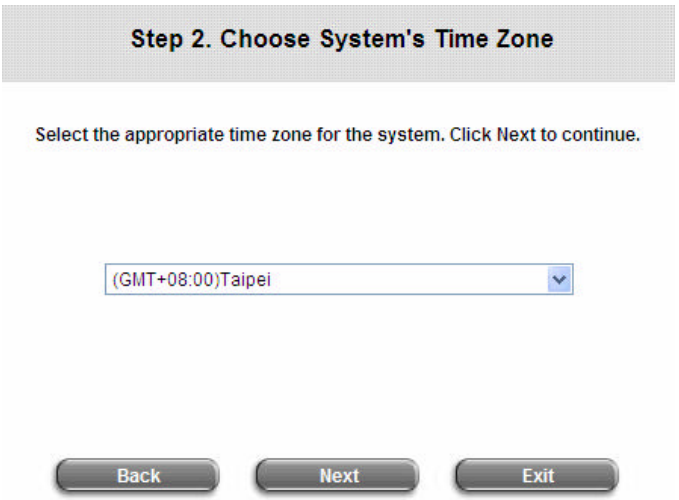

Configuration Wizard
Welcome to the Setup Wizard. The wizard will guide you through these 6 quick steps. Begin by clicking on Next.
Step 1. Change Admin's Password
Step 2. Choose System's Time Zone
Step 3. Set System Information
Step 4. Select the Connection Type for WAN Port
Step 5. Add Local User Account (Optional)
Step 6. Save and Restart WMS-208
Next
Exit

Note: *During every step of the wizard, if you wish to go back to modify the settings, please click the* ***Back*** *button to go back to the previous step.*

- **Step 1. Change Admin' s Password**
  - ➢ Enter a ***New Password*** for the admin account and retype it in the ***Verify Password*** field (20-character maximum and no spaces).
  - ➢ Click ***Next*** to continue.


Step 1. Change Admin's Password
You may change the Admin's account password by entering a new password. Click Next to continue.
New Password: •••••
Verify Password : •••••
Back
Next
Exit

- **Step 2. Choose System's Time Zone**
  - ➢ Select a proper time zone from the drop-down list box.
  - ➢ Click ***Next*** to continue.



- **Step 3. Set System Information**
  - **Home Page:** Enter the URL that users should be initially directed to when successfully authenticated to the network.
  - **NTP Server:** Enter the URL of the external time server for PheeNet WMS-208 time synchronization or use the default setting.
  - **DNS Server:** Enter the IP Address of a DNS Server provided by your ISP (Internet Service Provider). Contact the ISP if the DNS IP Address is unknown.
  - Click ***Next*** to continue.

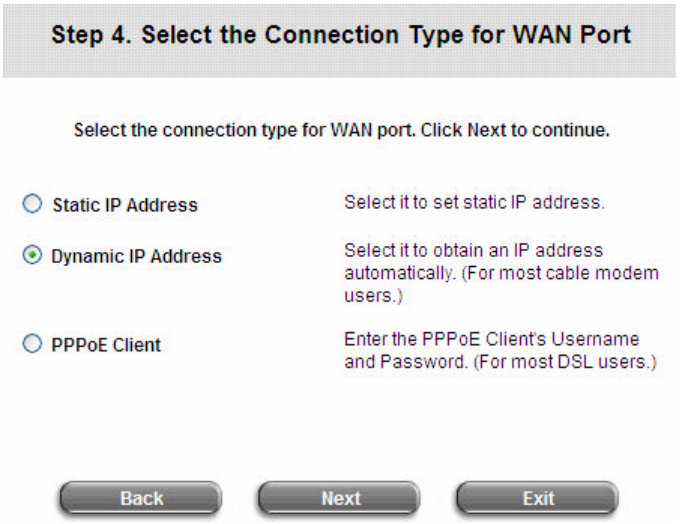
- **Step 4. Select Connection Type for WAN Port**

  Three are three types of WAN port to be selected from: **Static IP Address**, **Dynamic IP Address** and **PPPoE Client**. Select a proper Internet connection type and click ***Next*** to continue.

  - **Dynamic IP Address**

    If this option is selected, an appropriate IP address and related information will automatically be assigned.

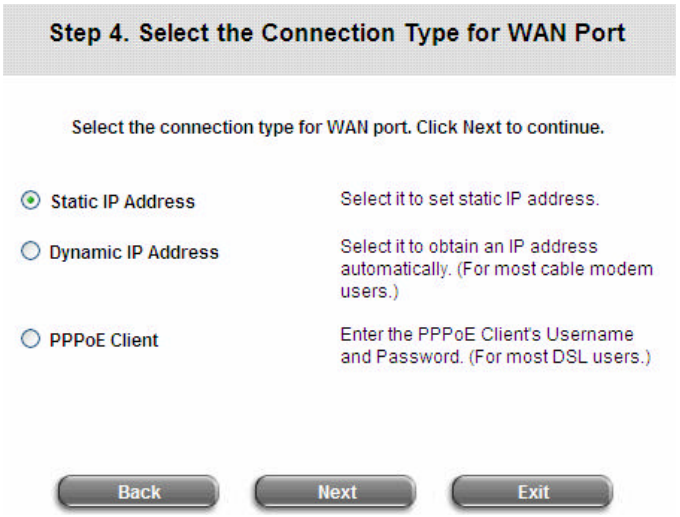
    Click ***Next*** to continue.


Step 4. Select the Connection Type for WAN Port
Select the connection type for WAN port. Click Next to continue.
Static IP Address
Select it to set static IP address.
Dynamic IP Address
Select it to obtain an IP address automatically. (For most cable modem users.)
PPPoE Client
Enter the PPPoE Client's Username and Password. (For most DSL users.)
Back
Next
Exit

- **Static IP Address: Set WAN Port's Static IP Address**

  Enter the **"IP Address"**, **"Subnet Mask"** and **"Default Gateway"** provided by your ISP.

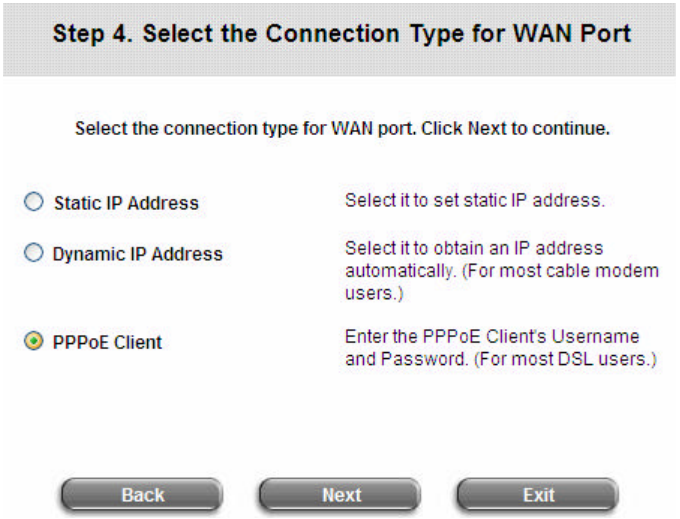
  Click ***Next*** to continue.

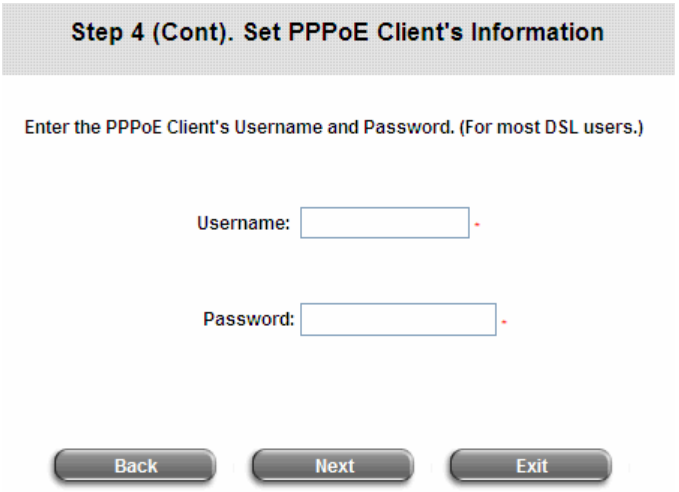

Step 4. Select the Connection Type for WAN Port
Select the connection type for WAN port. Click Next to continue.
Static IP Address
Select it to set static IP address.
Dynamic IP Address
Select it to obtain an IP address automatically. (For most cable modem users.)
PPPoE Client
Enter the PPPoE Client's Username and Password. (For most DSL users.)
Back
Next
Exit

- **PPPoE Client: Set PPPoE Client's Information**

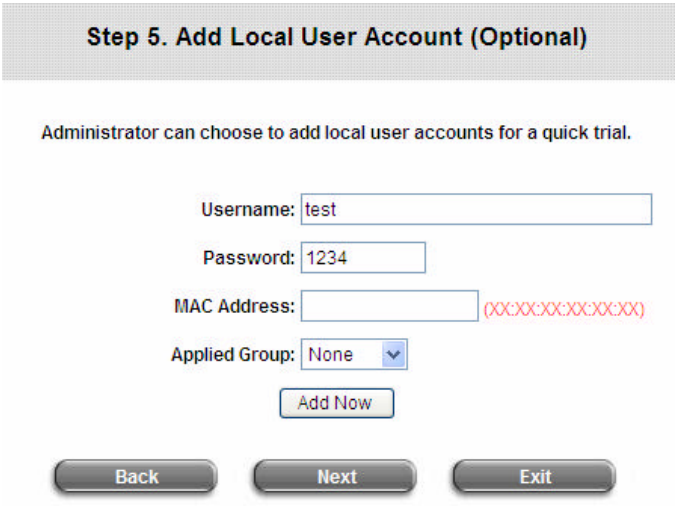
  Enter the **"Username"** and **"Password"** provided by the ISP.

  Click ***Next*** to continue.


Step 4. Select the Connection Type for WAN Port
Select the connection type for WAN port. Click Next to continue.
Static IP Address
Select it to set static IP address.
Dynamic IP Address
Select it to obtain an IP address automatically. (For most cable modem users.)
PPPoE Client
Enter the PPPoE Client's Username and Password. (For most DSL users.)
Back
Next
Exit



- **Step 5. Add Local User Account (Optional)**
  - A new user can be added to the Local User database. To add a user here, enter the ***Username*** (e.g. test), ***Password*** (e.g. test), ***MAC Address*** (optional) and assign an ***Applied Group*** to this particular user (or use the default **None**).
  - More users can be added to this authentication method by clicking the ***Add Now*** button.
  - Click ***Next*** to continue.

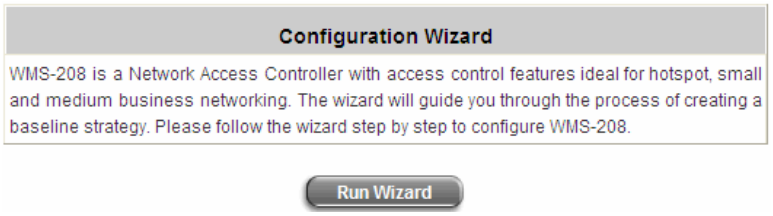


- **Step 6. Save and Restart PheeNet WMS-208**
  - Click ***Restart*** to save current settings and restart PheeNet WMS-208. The Setup Wizard is now complete.

Step 6. Save and Restart WMS-208
The Setup Wizard has completed. Click on Back to review or modify settings. Click Restart to save the settings and restart the system to have the current settings take effect.
Back
Restart
Exit

- **Restart:** When WMS-208 is restarting, a **"Restarting now. Please wait for a moment."** message will appear on the screen.

Please do NOT interrupt WMS-208 restart process until the Configuration Wizard pop-up window has disappeared—which indicates the restart process has been completed. If all steps are done properly, you can start working on the system or refer to the user's manual for advanced settings.


Configuration Wizard
WMS-208 is a Network Access Controller with access control features ideal for hotspot, small and medium business networking. The wizard will guide you through the process of creating a baseline strategy. Please follow the wizard step by step to configure WMS-208.
Run Wizard

Note: *For an example of user login, please refer to* ***Appendix F. Network Configuration on PC & User Login****.*

Chapter 4. Web Interface Configuration

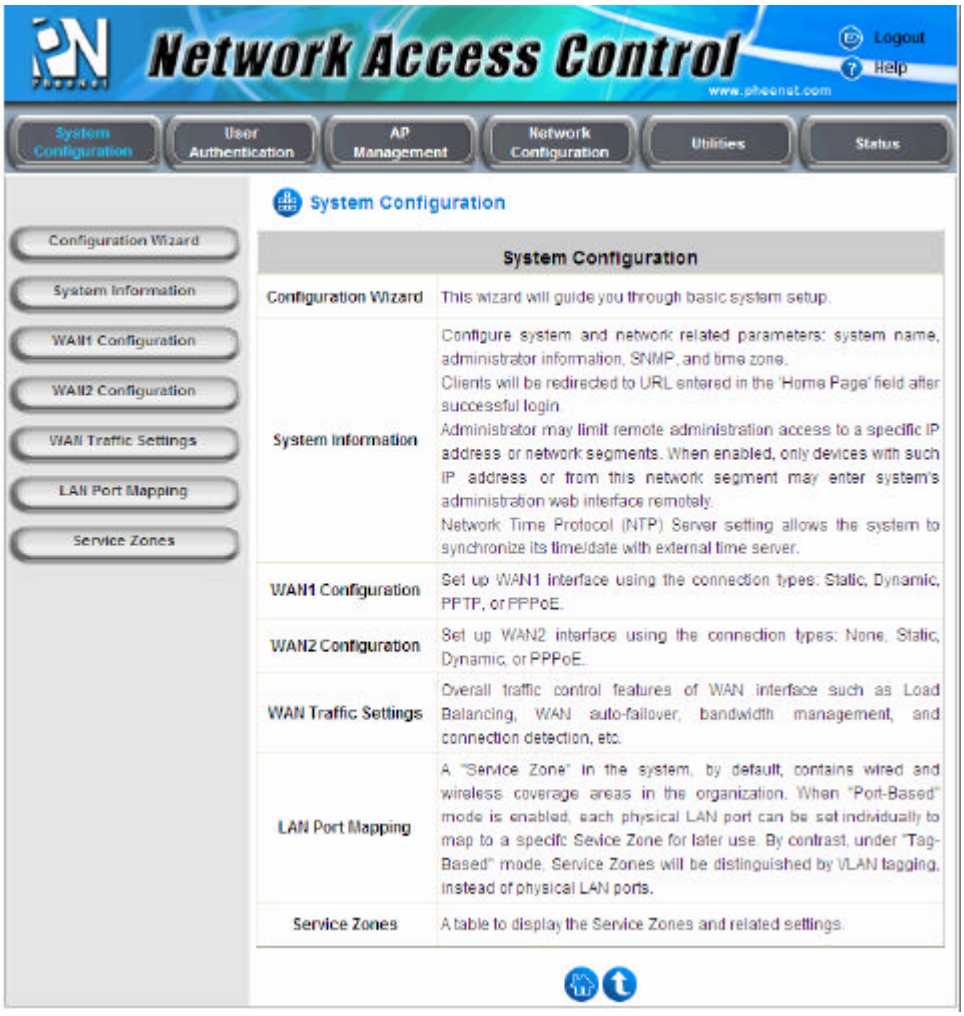
This chapter will guide you through further detailed settings. The following table is the UI and functions of the WMS-208.

OPTION	System Configuration	User Authentication	AP Management	Network Configuration	Utilities	Status
FUNCTION	Configuration Wizard	Authentication Configuration	AP List	Network Address Translation	Change Password	System Status
	System Information	Black List Configuration	AP Discovery	Privilege List	Backup/Restore Settings	Interface Status
	WAN1 Configuration	Group Configuration	Manual Configuration	Monitor IP List	Firmware Upgrade	Routing Table
	WAN2 Configuration	Policy Configuration	Template Settings	Walled Garden List	Restart	Current Users
	WAN Traffic Settings	Additional Configuration	Firmware Management	Proxy Server Properties	Network Utilities	Traffic History
	LAN Port Mapping		AP Upgrade	Dynamic DNS		Notification Configuration
	Service Zones		WDS Management	IP Mobility		
				VPN Configuration		

Caution: *After finishing the configuration of the settings, please click* ***Apply*** *and pay attention to see if a restart message appears on the screen. If such message appears, system must be restarted to allow the settings to take effect. All on-line users will be disconnected during restart.*

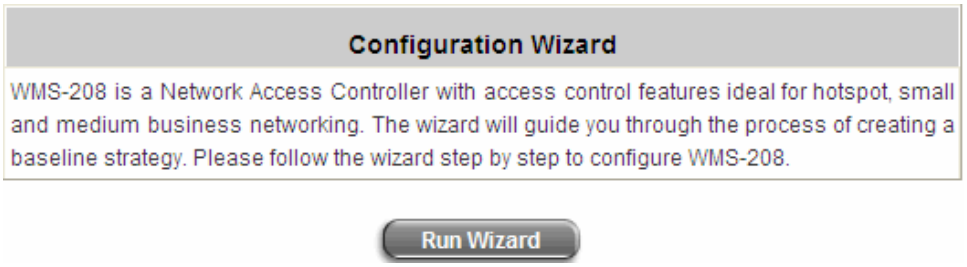
4.1 System Configuration

This section includes the following functions: **Configuration Wizard**, **System Information**, **WAN1 Configuration**, **WAN2 Configuration**, **WAN Traffic Settings**, **LAN Port Mapping** and **Service Zones**.


Network Access Control
www.pheenet.com
Logout
Help
System Configuration
User Authentication
AP Management
Network Configuration
Utilities
Status
Configuration Wizard
System Information
WAN1 Configuration
WAN2 Configuration
WAN Traffic Settings
LAN Port Mapping
Service Zones
System Configuration
System Configuration
Configuration Wizard
This wizard will guide you through basic system setup.
System Information
Configure system and network related parameters: system name, administrator information, SNMP, and time zone.
Clients will be redirected to URL entered in the 'Home Page' field after successful login.
Administrator may limit remote administration access to a specific IP address or network segments. When enabled, only devices with such IP address or from this network segment may enter system's administration web interface remotely.
Network Time Protocol (NTP) Server setting allows the system to synchronize its time/date with external time server.
WAN1 Configuration
Set up WAN1 interface using the connection types: Static, Dynamic, PPTP, or PPPoE.
WAN2 Configuration
Set up WAN2 interface using the connection types: None, Static, Dynamic, or PPPoE.
WAN Traffic Settings
Overall traffic control features of WAN interface such as Load Balancing, WAN auto-failover, bandwidth management, and connection detection, etc.
LAN Port Mapping
A "Service Zone" in the system, by default, contains wired and wireless coverage areas in the organization. When "Port-Based" mode is enabled, each physical LAN port can be set individually to map to a specific Sevice Zone for later use. By contrast, under "Tag-Based" mode, Service Zones will be distinguished by VLAN tagging, instead of physical LAN ports.
Service Zones
A table to display the Service Zones and related settings.

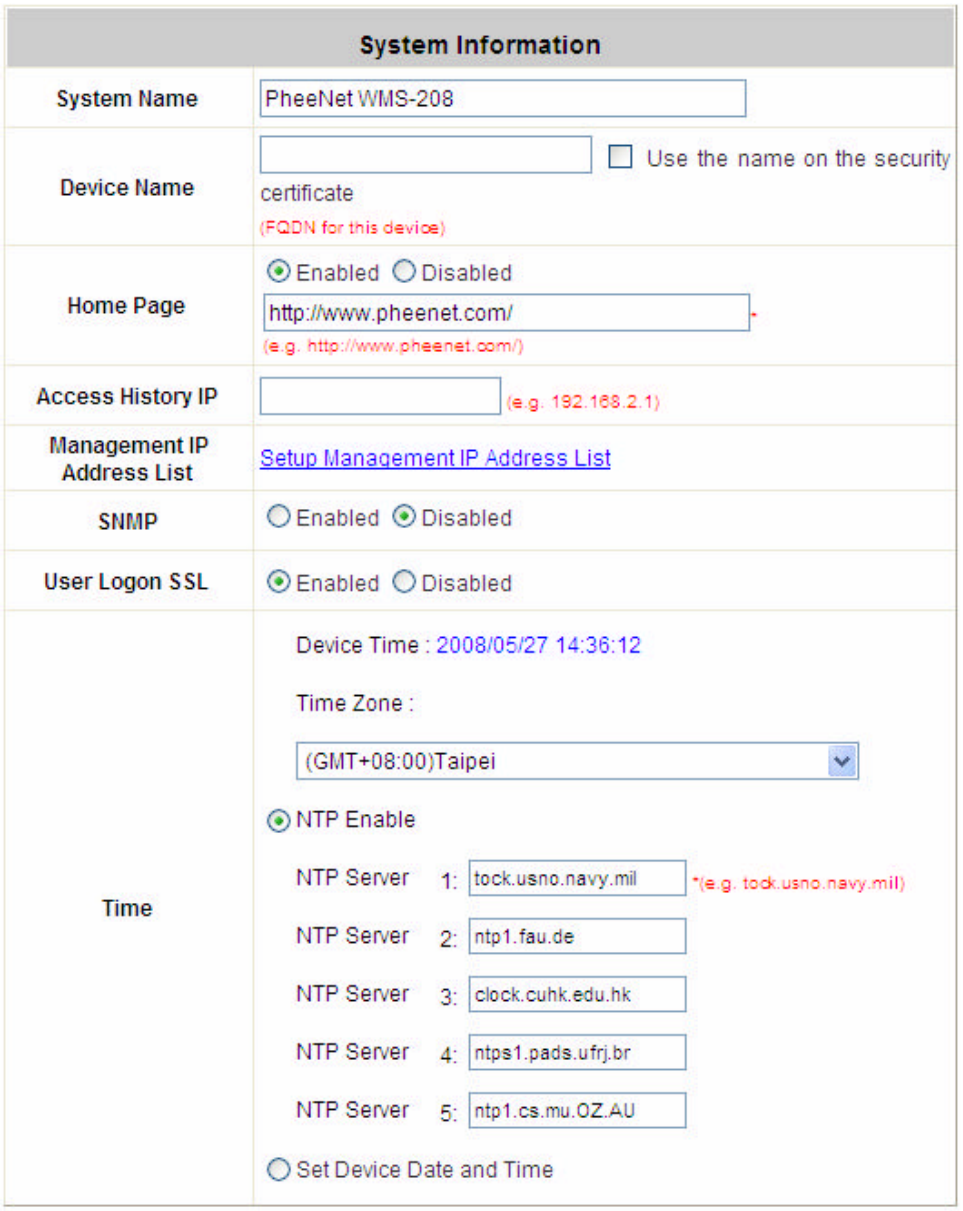
4.1.1 Configuration Wizard

There are two ways to configure the PheeNet WMS-208 system: using the online **Configuration Wizard** or changing the settings by commands manually. The **Configuration Wizard** comprises of 6 basic steps, providing a simple and easy way to go through the basic setups of WMS-208 and is served as **3.2 Quick Software Configuration**.


Configuration Wizard
WMS-208 is a Network Access Controller with access control features ideal for hotspot, small and medium business networking. The wizard will guide you through the process of creating a baseline strategy. Please follow the wizard step by step to configure WMS-208.
Run Wizard

4.1.2 System Information

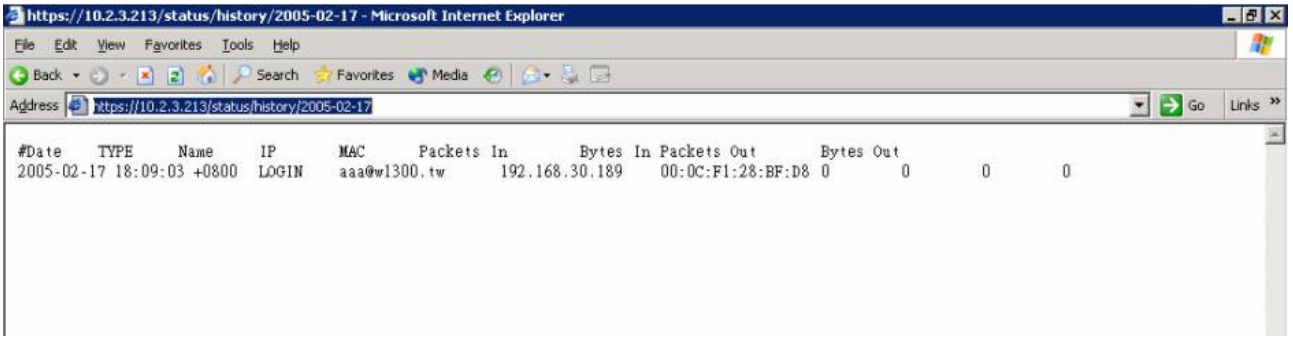
Main information about PheeNet WMS-208 is shown as follows:



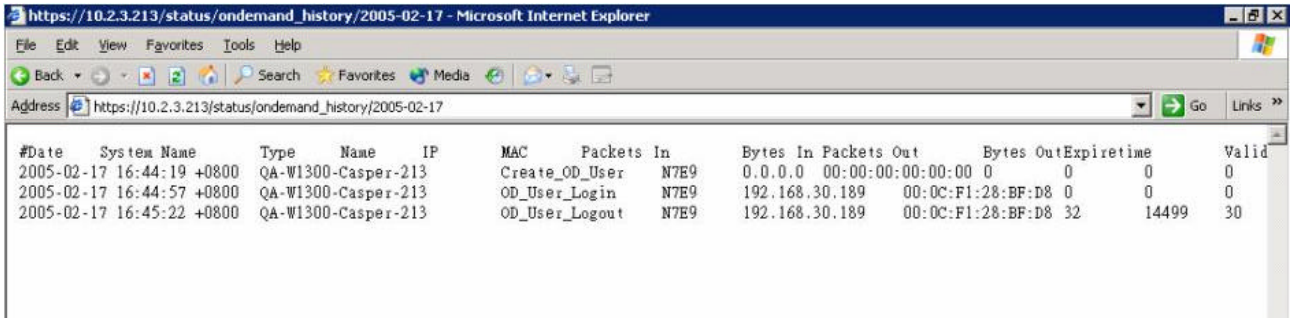
- **System Name:** Set the system's name or use the default name.
- **Device Name:** FQDN (Fully-Qualified Domain Name). This is the domain name of the WMS-208 as seen on client machines connected on LAN ports. A user on client machine can use this domain name to access WMS-208 instead of its IP address. In addition, when "***Use the name on the security certificate***" option is checked, the system will use the CN (Common Name) value of the uploaded SSL certificate as the domain name.
- **Home Page:** Enter the website of a Web Server to be the homepage. When users log in successfully, they will be directed to the homepage set. Usually, the homepage is set to the company's website, such as http://www.pheenet.com.tw/eng/. If the home page function is disabled, the user will be directed to the URL she/he tries to visit originally.
- **Access History IP:** Specify an IP address of the administrator's computer or a billing system to get billing

history information of WMS-208 with the predefined URLs as the following:

Traffic History：https://10.2.3.213/status/history/2005-02-17

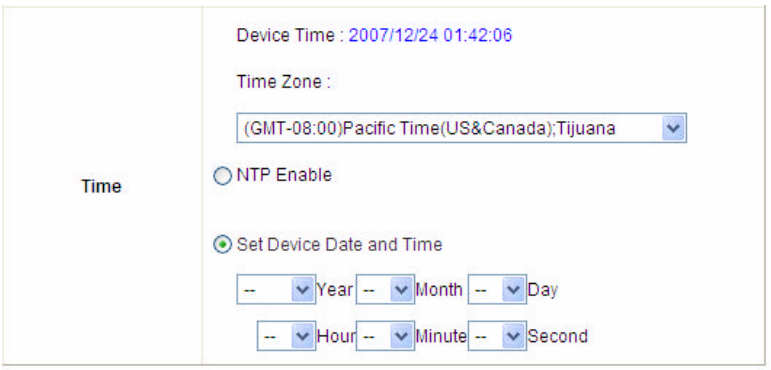

https://10.2.3.213/status/history/2005-02-17 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://10.2.3.213/status/history/2005-02-17
Go Links
#Date TYPE Name IP MAC Packets In Bytes In Packets Out Bytes Out
2005-02-17 18:09:03 +0800 LOGIN aaa@w1300.tw 192.168.30.189 00:0C:F1:28:BF:D8 0 0 0 0

On-demand History：https://10.2.3.213/status/ondemand_history/2005-02-17


https://10.2.3.213/status/ondemand_history/2005-02-17 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://10.2.3.213/status/ondemand_history/2005-02-17
Go Links
#Date System Name Type Name IP MAC Packets In Bytes In Packets Out Bytes Out Expiretime Valid
2005-02-17 16:44:19 +0800 QA-W1300-Casper-213 Create_OD_User N7E9 0.0.0.0 00:00:00:00:00:00 0 0 0 0
2005-02-17 16:44:57 +0800 QA-W1300-Casper-213 OD_User_Login N7E9 192.168.30.189 00:0C:F1:28:BF:D8 0 0 0
2005-02-17 16:45:22 +0800 QA-W1300-Casper-213 OD_User_Logout N7E9 192.168.30.189 00:0C:F1:28:BF:D8 32 14499 30

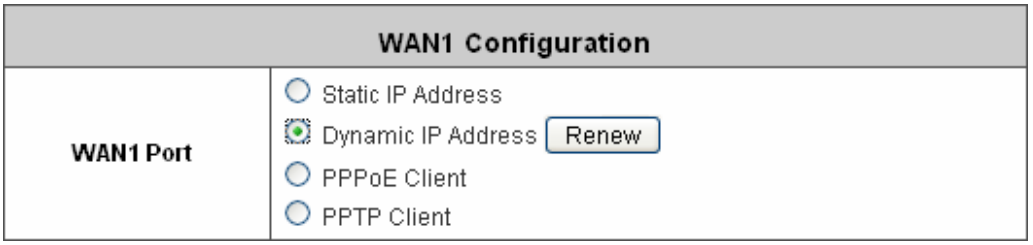
- **Management IP Address List:** In the page of "Management IP Address List", the administrator can grant the access of the web management interface by specifying a list specific IP addresses or ranges of IP addresses, no matter the access is from WAN or LAN.
- **SNMP:** If the function is enabled, the Manager IP and the community can be assigned to access the management information base (MIB) of the system.

  User Logon SSL: Enable to activate https (encryption) or disable to activate http (non encryption) login page.
- **Time:** WMS-208 supports NTP (Network Time Protocol) communication protocol to synchronize the network time. Please specify the IP address of a NTP server to adjust the time automatically (Universal Time is Greenwich Mean Time, GMT). The time can also be set manually by selecting **"Set Device Date and Time"** and then entering the date and time in these fields.

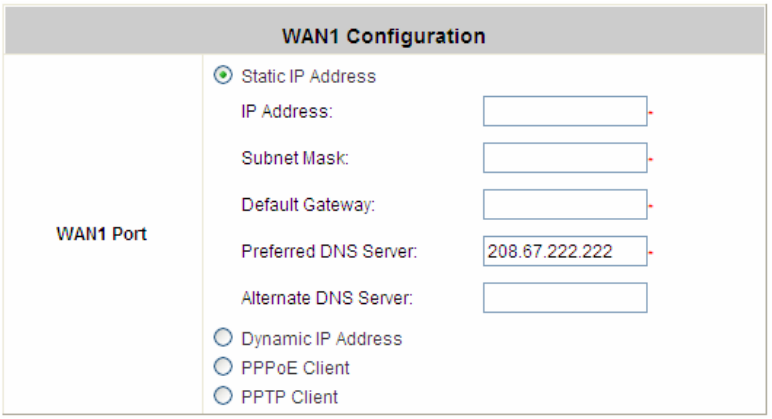


4.1.3 WAN1 Configuration

There are 4 methods of obtaining IP address for the WAN Port: **Static IP Address**, **Dynamic IP Address**, **PPPoE** and **PPTP Client**.



- **Static IP Address:** Manually specifying the IP address of the WAN port. The red asterisks indicate required fields to be filled in.



IP address: the IP address of the WAN1 port.

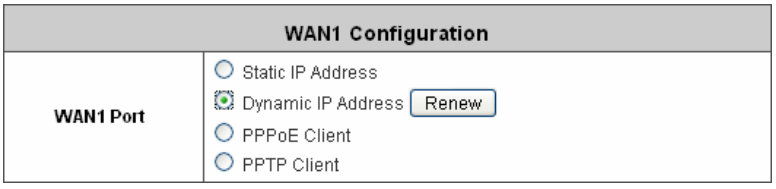
Subnet mask: the subnet mask of the network WAN1 port connects to.

Default gateway: a gateway of the network WAN1 port connects to.

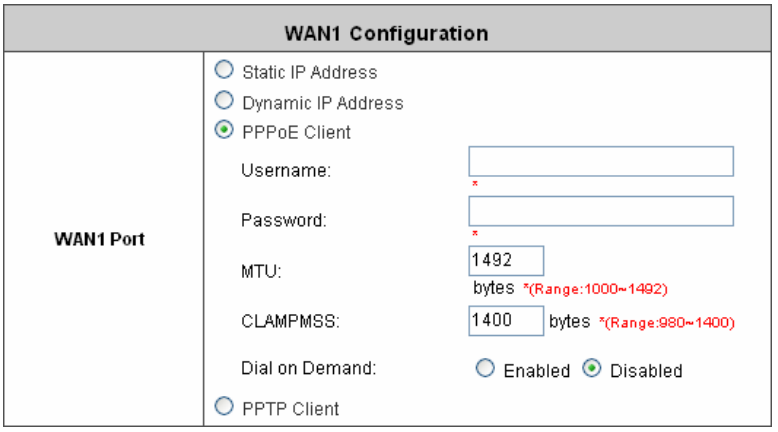
Preferred DNS Server: The primary DNS server is used by the system.

Alternate DNS Server: The substitute DNS server is used by the system. This is an optional field.

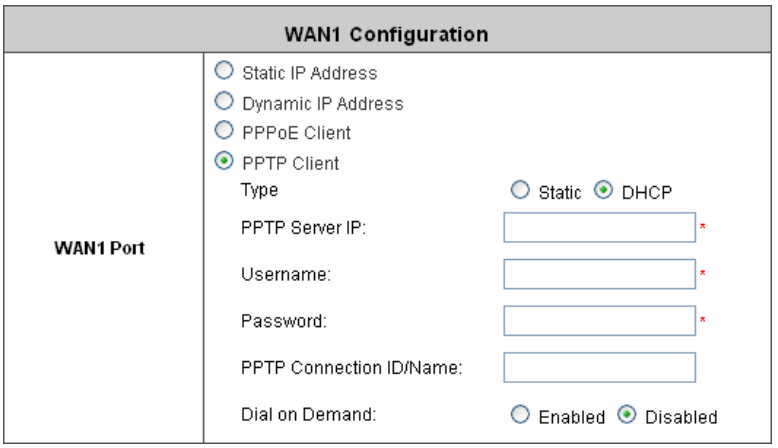
- **Dynamic IP Address:** It is only applicable for the network environment where the DHCP server is available on the network. Click the ***Renew*** button to get an IP address automatically.



- **PPPoE Client:** When selecting PPPoE to connect to the network, please set the **"Username"**, **"Password"**, **"MTU"** and **"CLAMPMSS"**. There is a **Dial on demand** function under PPPoE. If this function is enabled, a **Maximum Idle Time** can be set. When the idle time is reached, the system will automatically disconnect itself.

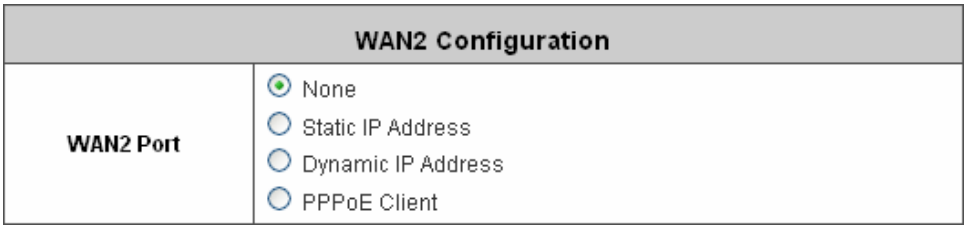


- **PPTP Client:** Select **STATIC** to specify the IP address of the PPTP Client manually or select **DHCP** to get the IP address automatically. The fields with red asterisks are required to be filled in. There is a **Dial on demand** function under PPPoE. If this function is enabled, a **Maximum Idle Time** can be set. When the idle time is reached, the system will automatically disconnect itself.

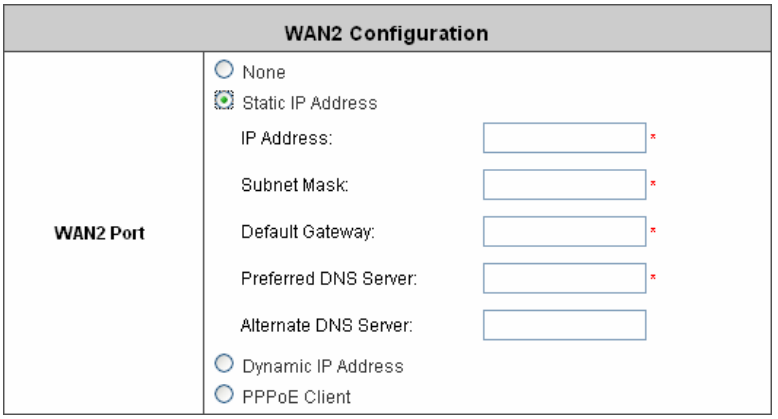


4.1.4 WAN2 Configuration

Select **None** to disable this WAN2 interface, or there are 3 connection types for the WAN2 port: **Static IP Address, Dynamic IP Address,** and **PPPoE Client**.



- **None**: The WAN2 Port is disabled.
- **Static IP Address:** Manually specifying the IP address of the WAN port. The red asterisks indicate required fields to be filled in.



IP Address: the IP address of the WAN2 port.

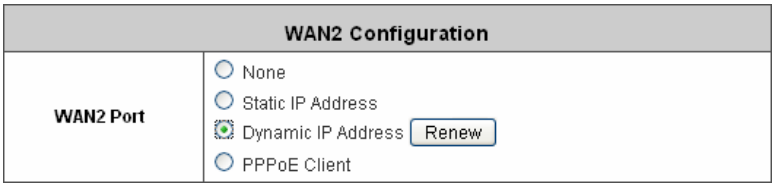
Subnet Mask: the subnet mask of the network WAN2 port connects to.

Default Gateway: a gateway of the network WAN2 port connects to.

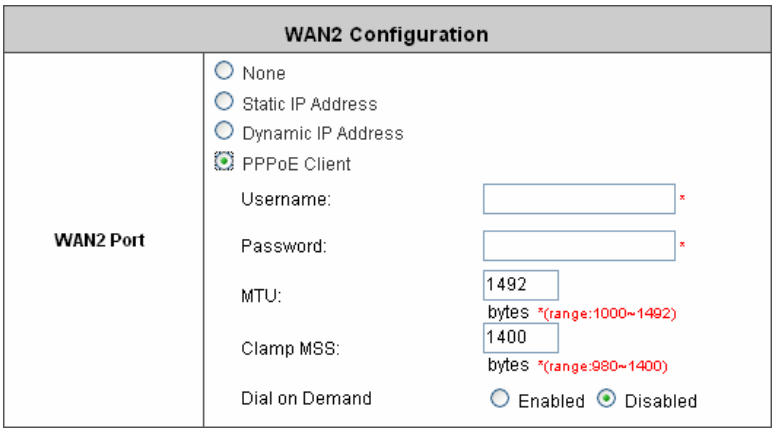
Preferred DNS Server: The primary DNS server is used by the system.

Alternate DNS Server: The substitute DNS server is used by the system. This is an optional field.

- **Dynamic IP Address:** It is only applicable for the network environment where a DHCP server is available. Click the ***Renew*** button to get an IP address.

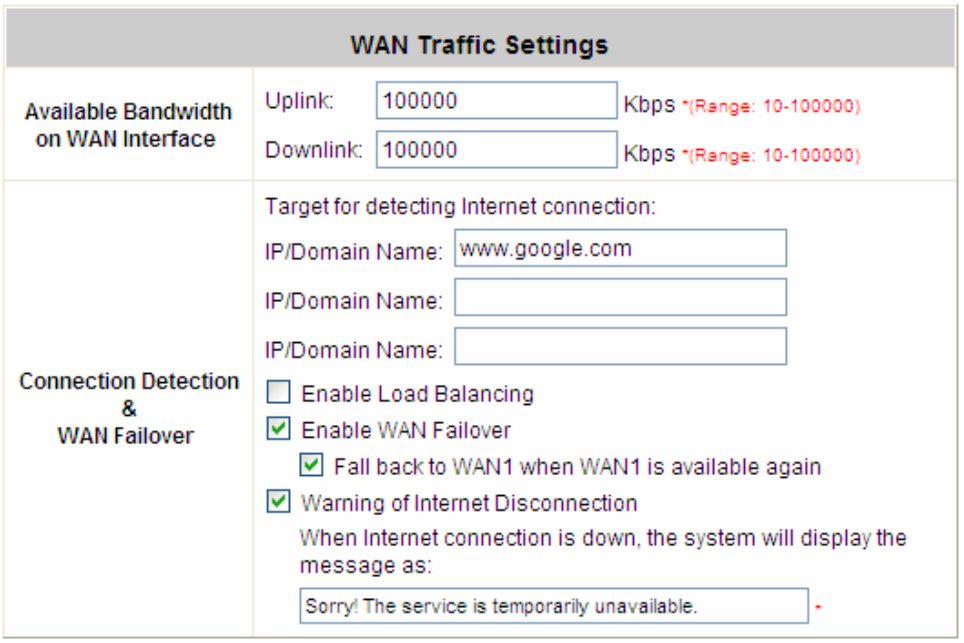


- **PPPoE Client:** When selecting PPPoE to connect to the network, please set the **"UserName"** and **"Password"**. There is a **Dial on demand** function under PPPoE. If this function is enabled, **Maximum Idle Time can be set**. When the idle time is reached, the system will automatically disconnect itself.



4.1.5 WAN Traffic Settings

The section is for administrators to configure the control over the entire system's traffic though the WAN interface (WAN1 and WAN2 ports).


WAN Traffic Settings
Available Bandwidth on WAN Interface
Uplink: 100000 Kbps *(Range: 10-100000)
Downlink: 100000 Kbps *(Range: 10-100000)
Connection Detection & WAN Failover
Target for detecting Internet connection:
IP/Domain Name: www.google.com
IP/Domain Name:
IP/Domain Name:
Enable Load Balancing
Enable WAN Failover
Fall back to WAN1 when WAN1 is available again
Warning of Internet Disconnection
When Internet connection is down, the system will display the message as:
Sorry! The service is temporarily unavailable.

Available Bandwidth on WAN Interface:

- **Uplink:** It specifies the maximum uplink bandwidth that can be shared by clients of the system.
- **Downlink:** It specifies the maximum downlink bandwidth that can be shared by clients of the system.

Connection Detection & WAN Failover:

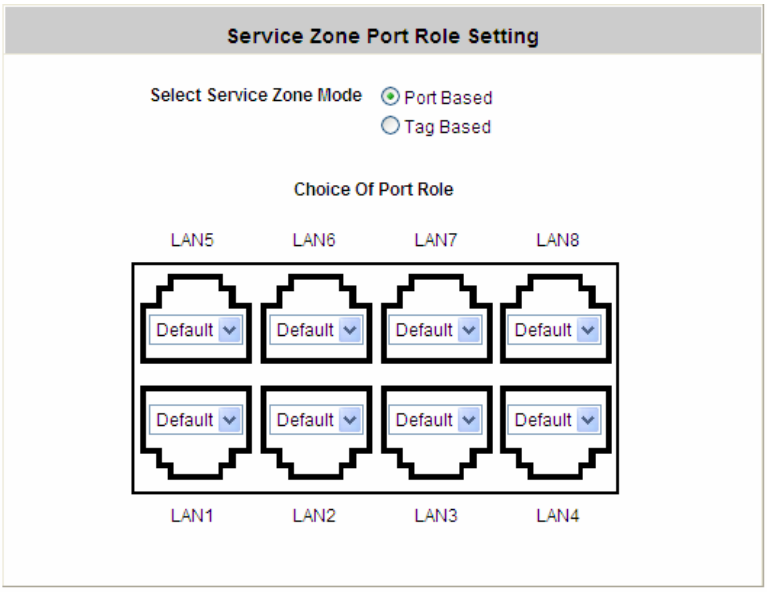
- **Target for detecting Internet connection:** These URLs are used by the system as the targets to detect Internet connection, for alerting Internet disconnection and WAN Failover. At least one URL is required to enable WAN Failover.
- **Enable Load Balancing:** Outbound load balancing is supported by the system. When enabled, the system will allocate traffic between WAN1 and WAN2 dynamically according to designed algorithms based on the weight ratio.
  - **WAN1 Weight:** The percentage of traffic through WAN1. (Range: 1~99; by default, it is 50)
  - **Base:** The weight ratio between WAN1 and WAN2 can be based on Sessions, Packets or Bytes. Packets and Bytes are based on historic data. New connection sessions will be distributed between WAN1 and WAN2 by a weight ratio using random number.
- **Enable WAN Failover:** Normally a Service Zone uses WAN1 as it primary WAN interface. When enabled and WAN2 is available, WAN1's traffic will be routed to WAN2 when WAN1 connection is down. On the other hand, a Service Zone's policy could also use WAN2 as its interface; in that case, if WAN2 is down, the WAN2's traffic under its policy will also be routed to WAN1.
  - **Fall back to WAN1 when WAN1 is available again:** If WAN Failover is enabled, the traffic will be routed to WAN2 automatically when WAN1 connection fails. When **fall back to WAN1** is enabled, the routed traffic will be connected back to WAN1 when WAN1 connection is recovered.

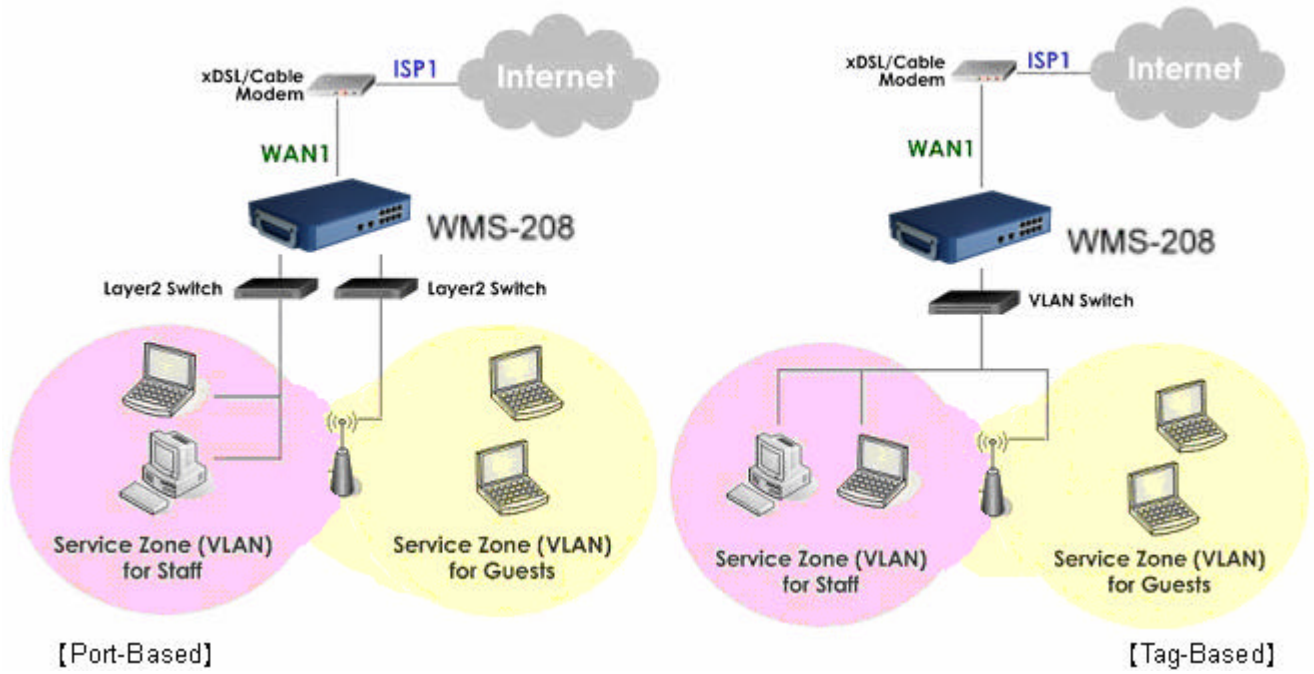
- **Warning of Internet Disconnection:** When enabled, there is a text box available for the administrator to enter a reminding message. This reminding message will appear on clients' screens when Internet connection is down.

***Note: SIP authentication** is exempt from **Load Balancing** and **WAN Failover**. A fixed WAN port is used for SIP traffic.*

4.1.6 LAN Port Mapping

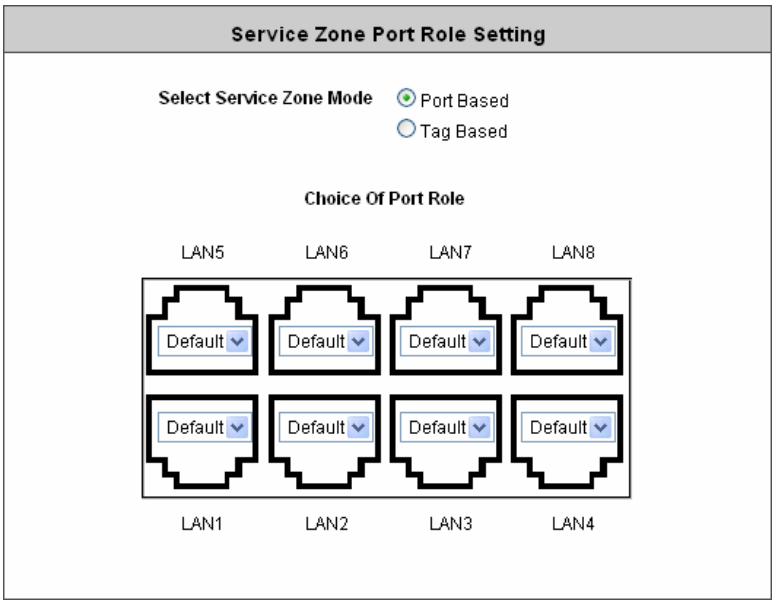
WMS-208 supports multiple Service Zones in either of the two VLAN modes, **Port-Based** or **Tag-Based**, but not concurrently. In **Port-Base** mode, each LAN port can only serve traffic from one Service Zone as each Service Zone is identified by physical LAN ports. In **Tag-Based** mode, each LAN port can serve traffic from any Service Zone as each Service Zone is identified by VLAN tags carried within message frames. **By default, the system is in Port-Based mode with Default Service Zone enabled and all LAN ports are mapped to Default Service Zone.** Compare the two figures below to see the differences.





It is recommended that the administrator decides which mode is better for a multiple-service-zone deployment before proceeding further with the system configuration. Settings for the two VLAN modes are slightly different, for example, the VLAN Tag setting is required for Tag-Based mode.

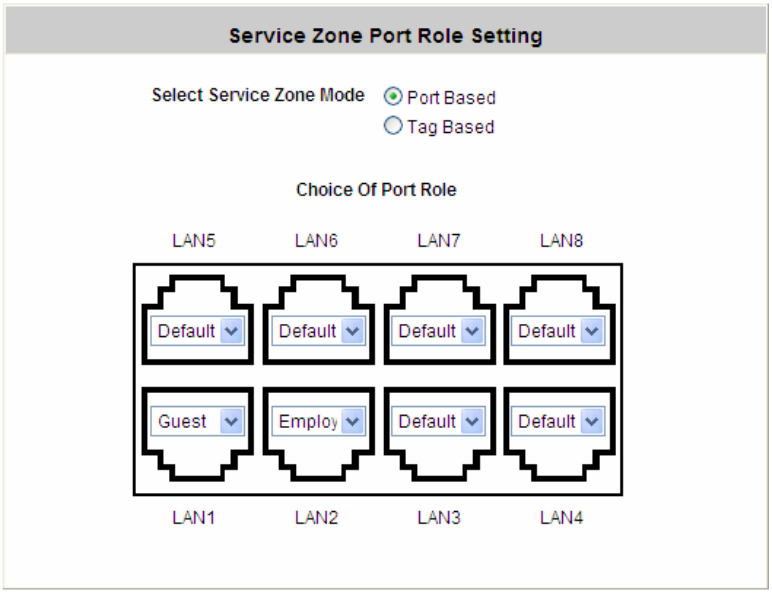
- **Select Service Zone Mode**: Select a VLAN mode, either ***Port-Based*** or ***Tag-Based***.



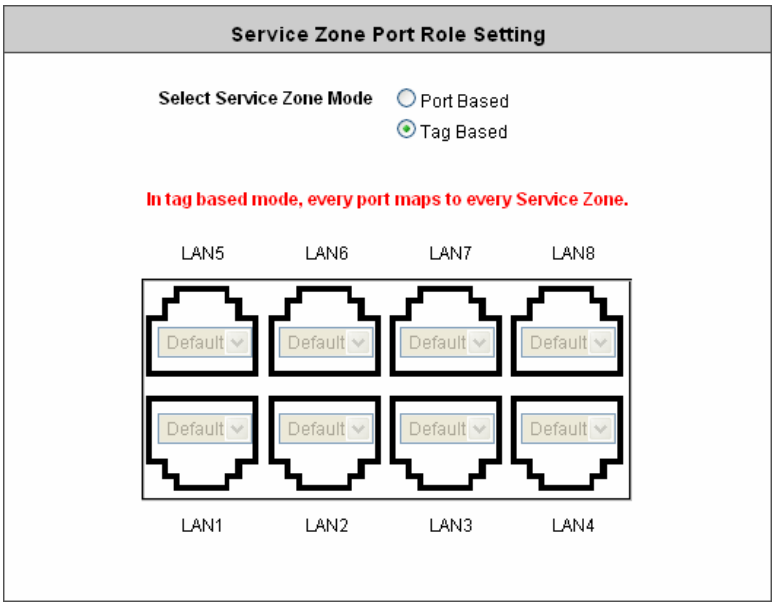
Note: *The switches deployed under WMS-208 in* ***Port-Based*** *mode must be* ***Layer 2 switches*** *only.*
The switch deployed under WMS-208 in ***Tag-Based*** *mode must be a* ***VLAN switch*** *only.*

- **Port-Based:** When Port-Based mode is selected, traffic from different virtual Service Zones will be distinguished by physical LAN ports. Each LAN port can be mapped to a Service Zone in the form of a many-to-one mapping between ports and Service Zones.

  - **Specify a desired Service Zone for each LAN Port:** For each LAN port, select a Service Zone to which the LAN port is to be mapped from the drop-down list box.
    By factory default, all LAN ports are mapped to Default Service Zone; therefore, the administrator can enter the web management interface via any LAN port upon the first power up of the system. From the drop-down list box, all disabled Service Zones are gray-out; to activate any desired Service Zone, please configure the desired Service Zone under the **Service Zone** tab and enable its *Service Zone Status* (refer to **Section 4.1.7. Service Zones**).



- **Tag-Based:** When the Tag-Based mode is selected, traffic from different virtual Service Zones will be distinguished by VLAN tagging, instead of by physical LAN ports.
  Select *Tag-Based* and then click ***Apply*** to activate the Tag-Based VLAN function. When a restart message screen appears, do NOT restart the system until you have completed the configuration under the **Service Zones** tab first.



Note: *For more information on enabling and configuring Service Zones, please refer to* ***Appendix C. Service Zone Deployment Example****.*

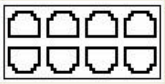
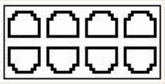
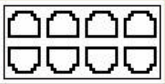
4.1.7 Service Zones

A *Service Zone* is a logical network area to cover certain wired and wireless networks in an organization such as SMB or branch offices. Service Zones can be set up as port-based or tag-based. For example, using a tag-based method to deploy Service Zones, by associating a unique VLAN Tag and SSID with each Service Zone, administrators can separate one physical network into different logical zones. Users attempting to access the resources within a particular Service Zone will be controlled based on the group they belong to and the group's associated policy profile, such as authentication methods, security features, wireless encryption methods, traffic control, and etc.

There are up to eight Service Zones plus one default zone to be utilized; by default, they are named as: **Default**, **SZ1~SZ8** , as shown in the two tables below.

- ***Port-based Service Zone:***

Service Zone Settings

Service Zone Name	Port Map	SSID	WLAN Encryption	Applied Policy	Default Authentication	Status	Details
Default		PheeNet 0	None	Policy 1	Server 1	Enable	Configure
SZ1		PheeNet 1	None	Policy 1	Server 1	Disable	Configure
SZ2		PheeNet 2	None	Policy 1	Server 1	Disable	Configure
SZ3		PheeNet 3	None	Policy 1	Server 1	Disable	Configure
SZ4		PheeNet 4	None	Policy 1	Server 1	Disable	Configure
SZ5		PheeNet 5	None	Policy 1	Server 1	Disable	Configure
SZ6		PheeNet 6	None	Policy 1	Server 1	Disable	Configure
SZ7		PheeNet 7	None	Policy 1	Server 1	Disable	Configure
SZ8		PheeNet 8	None	Policy 1	Server 1	Disable	Configure

- **Service Zone Name:** Mnemonic name of the Service Zone.
- **Port Map:** Shows which port maps to which Service Zone in port-based mode.
- **SSID:** The SSID that is associated with the Service Zone.
- **WLAN Encryption:** Data encryption method for wireless networks within the Service Zone.
- **Applied Policy:** The **global policy** that is applied to the Service Zone. This is for users who are not assigned to any group such as users who access the network using Walled Garden. Each group can set its own **group policy**. **Group policy overrides global Service Zone policy.**

- ***Tag-based Service Zone:***

Service Zone Settings							
Service Zone Name	VLAN Tag	SSID	WLAN Encryption	Applied Policy	Default Authentication	Status	Details
Default	--	PheeNet0	None	Policy 1	Server 1	Enable	Configure
SZ1	1	PheeNet1	None	Policy 1	Server 1	Disable	Configure
SZ2	2	PheeNet2	None	Policy 1	Server 1	Disable	Configure
SZ3	3	PheeNet3	None	Policy 1	Server 1	Disable	Configure
SZ4	4	PheeNet4	None	Policy 1	Server 1	Disable	Configure
SZ5	5	PheeNet5	None	Policy 1	Server 1	Disable	Configure
SZ6	6	PheeNet6	None	Policy 1	Server 1	Disable	Configure
SZ7	7	PheeNet7	None	Policy 1	Server 1	Disable	Configure
SZ8	8	PheeNet8	None	Policy 1	Server 1	Disable	Configure

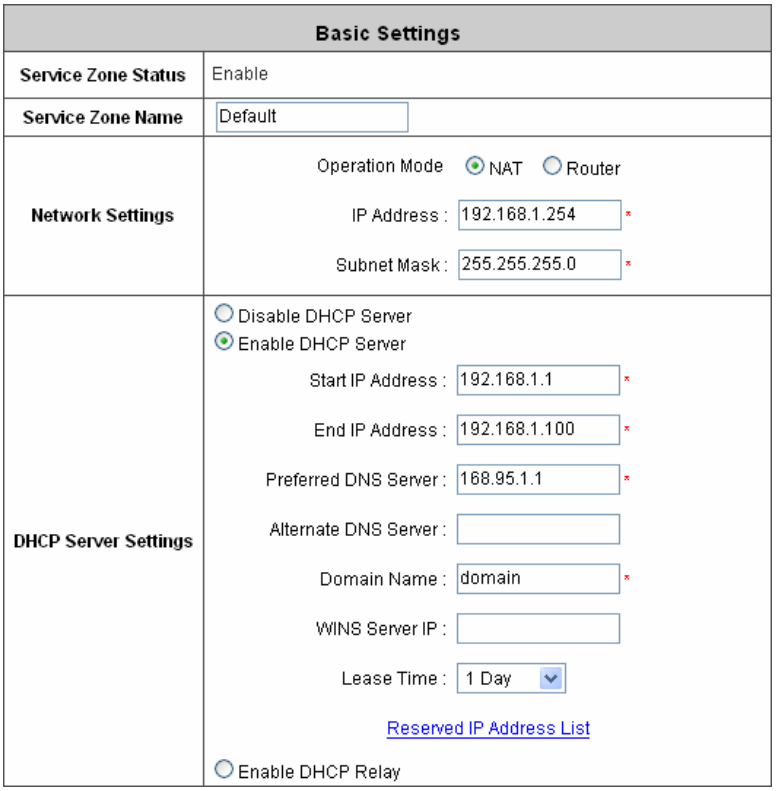
- **Service Zone Name:** Mnemonic name of the Service Zone.
- **VLAN Tag:** The VLAN tag number that is mapped to the Service Zone in tag-based mode.
- **SSID:** The SSID that is associated with the Service Zone.
- **WLAN Encryption:** Data encryption method for wireless networks within the Service Zone.
- **Applied Policy:** The **global policy** that is applied to the Service Zone. This is for users who are not assigned to any group such as users who access the network using Walled Garden. Each group can set its own **group policy**. **Group policy overrides global Service Zone policy.**

Note: *For more information about Group, please refer to* ***4.2.3 Group Configuration*** *section.*

- **Default Authentication:** Default authentication method/server that is used within the Service Zone.
- **Status:** Each Service Zone can be enabled or disabled.
- **Details:** Configurable, detailed settings for each Service Zone.

Click ***Configure*** button to configure each Service Zone: **Basic Settings**, **SIP Interface Configuration**, **Authentication Settings**, **Wireless Settings**, and **Managed AP in Each Service Zone**.

1) *Service Zone Settings – Basic Settings*



- **Service Zone Status:** Each service zone can be enabled or disabled except for the default service zone.
- **Service Zone Name:** The name of service zone could be input here.
- **Network Settings:**
  - **Operation Mode:** Contains **NAT** mode and **Router** mode. When NAT mode is chosen, the service zone runs in NAT mode. When Router mode is chosen this service zone runs in Router mode.
  - **IP address:** The IP Address of this service zone.
  - **Subnet Mask:** The subnet Mask of this service zone.
- **DHCP Server Settings:** Related information needed on setting up the DHCP Server is listed here. Please note that when "*Enable DHCP Relay*" is enabled, the IP address of clients will be assigned by an external DHCP server. The system will only relay DHCP information from the external DHCP server to downstream clients of this service zone.
  - **Start IP Address / End IP Address:** A range of IP addresses that built-in DHCP server will assign to clients. Note: please change the Management IP Address List accordingly (at *System Configuration >> System Information >> Management IP Address List*) to permit the administrator to access the WMS-208 admin page after the default IP address of the network interface is changed.
  - **Preferred DNS Server:** The primary DNS server that is used by this Service Zone.
  - **Alternate DNS Server:** The substitute DNS server that is used by this Service Zone.
  - **Domain Name:** Enter the domain name for this service zone.
  - **WINS Server IP:** The IP address of the WINS (Windows Internet Naming Service) server that if WINS server is applicable to this service zone.
  - **Lease Time:** This is the time period that the IP addresses issued from the DHCP server are valid

and available.

- **Reserved IP Address List:** Each service zone can reserve up to 40 IP addresses from predefined DHCP range to prevent the system from issuing these IP addresses to downstream clients. The administrator can reserve a specific IP address for a special device with certain MAC address.

2) *Service Zone Settings – SIP Interface Configuration*

SIP Interface Configuration		
Enabled ☑	WAN Interface	WAN1

The system provides SIP proxy functionality, which allows SIP clients to pass through NAT. When enabled, all SIP traffic can pass through NAT via a fixed WAN interface. The policy route setting of SIP Authentication must be configured carefully because it must cooperate with the fixed WAN interface for SIP authentication.

SIP Transparent Proxy can be activated in both NAT and Router mode. SIP Authentication must support in either mode. For users logging in through SIP authentication, a policy can be chosen to govern SIP traffic. The policy's login schedule profile will be ignored for SIP authentication. Specific route and firewall rules of the chosen policy will be applied to SIP traffic.

3) *Service Zone Settings – Authentication Settings*

Authentication Settings					
Authentication Status	○ Enable ◉ Disable				
Authentication Options	Auth Option	Auth Database	Postfix	Default	Enabled
	Server 1	LOCAL	local	◉	☑
	Server 2	POP3	pop3	○	☑
	Server 3	RADIUS	radius	○	☑
	Server 4	LDAP	ldap	○	☑
	On-demand User	ONDEMAND	guest	○	☑
	SIP	SIP	N/A		☐
Custom Pages	Login Page				Configure
	Logout Page				Configure
	Login Success Page				Configure
	Login Success Page for On-demand User				Configure
	Logout Success Page				Configure
Group Permission for this Service Zone	Configure				
Default Policy in this Service Zone	Policy 1	Edit System Policies			
Email Message for Login Reminding	◉ Enable ○ Disable	Edit Mail Message			

- **Authentication Status:** When enabled, users must be authenticated before they get access to the network within this Service Zone.
- **Authentication Options:** There are total seven types of authentication database (LOCAL, POP3, RADIUS, LDAP, NTDOMAIN, ONDEMAND, and SIP) that are supported by the entire system. For each Service Zone, up to six authentication options can be enabled, and one of them can be set as the default option – so that users do not have to type in the postfix string while entering username during login.
- **Custom Pages:** Related login and logout pages can be customized by administrators for each service zone. Please refer to ***Appendix I. Customizable Pages*** for more details.
- **Group Permission for this Service Zone:**

  For each Service Zone, the administrator can set up multiple groups for that Service Zone. For each group, an associated policy can be assigned. Therefore, users in the same group follow the same policy and have the same privileges.

  To configure Group permission based on the role of this Service Zone.

  Click ***Configure*** to have further configuration or view the details.

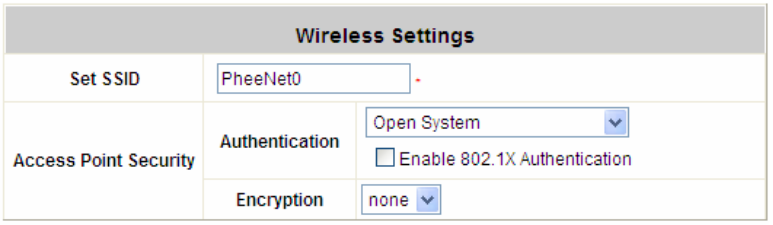
  Click ***Enabled*** of the desired Group option(s) to allow the clients of the selected Group(s) to log into this Service Zone after a successful authentication. Moreover, a pre-defined Policy can be applied to any Group in this Service Zone.

  Click the hyperlink of the respective Group names in the **Edit Group Option** column to enter the **Group Configuration** tab, where zone permission and policy assignment can be further configured (refer to **Section 4.2.3. Group Configuration**).

Group Permission - Service Zone : Default			
Group Option	Enabled	Policy	Edit Group Option
Group 1	☑	Policy 1	Group 1
Group 2	☑	Policy 2	Group 2
Group 3	☑	Policy 3	Group 3
Group 4	☑	Policy 4	Group 4
Group 5	☑	Policy 5	Group 5
Group 6	☑	Policy 6	Group 6
Group 7	☑	Policy 7	Group 7
Group 8	☑	Policy 8	Group 8

- **Default Policy in this Service Zone:** For each Service Zone, one policy can be applied to enforce the access control over the users. Please refer to ***4.2.4 Policy Configuration*** for complete description.
- **Email Message for Login Reminding:** When enabled, the system will automatically send an email to users if they attempt to send/receive their emails using POP3 email program (for example, Microsoft Outlook) before they are authenticated. Click ***Edit Mail Message*** to edit the message in HTML format:

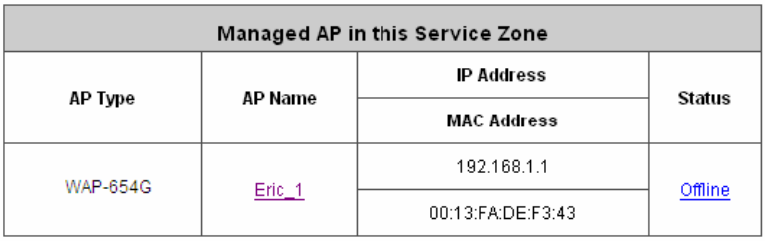
4) *Service Zone Settings – Wireless Settings*



- **Set SSID:** Each service zone can be mapped with its own SSID.
- **Access Point Security:** For each service zone, administrators can set up the wireless security profile, including **Authentication** and **Encryption**.

5) *Service Zone Settings – Managed AP in this Service Zone*

All managed APs that belong to this service zone are listed here.



4.2 User Authentication

This section includes the following functions: **Authentication Configuration**, **Black List Configuration**, **Group Configuration**, **Policy Configuration** and **Additional Configuration**.

Network Access Control
www.pheenet.com
Logout
Help
System Configuration
User Authentication
AP Management
Network Configuration
Utilities
Status
Authentication Configuration
Black List Configuration
Group Configuration
Policy Configuration
Additional Configuration
User Authentication
User Authentication
Authentication Configuration
Each server allows only one type of authentication method and one Black List Profile. System supports the following external authentication servers: POP3(S), RADIUS, LDAP, NT Domain and SIP.
Black List Configuration
System supports 5 Black List profiles for used within the authentication server. On-demand users are NOT bounded by the Black List.
Group
8 sets of group profiles can be define and used to enforce the access control for different groups of users.
Policy Configuration
A policy can be selected to apply to a group of users within a zone. 12 sets of policy profiles including Firewall Profile, Specific Route Profile, Schedule Profile, and Session Limit Management can be defined.
Additional Configuration
Additional configurations are in this section. They are User Session Control, Built-in RADIUS Server Settings, Customization, Remaining Time Reminder, and MAC ACL. The administrator can control user session such as idle timeout in User Session Control. Three fuctions are provided in Built-in RADIUS Server Settings such as session timeout. In Customization, the administrator can upload certificate to the system. Remaining Time Reminder provides remaining time information to clients on the screen. The administrator can manage the access control to the system via clients' MAC address in the MAC ACL(Access Control List).

4.2.1 Authentication Configuration

This section is for administrators to pre-configure authentication servers for the entire system's Service Zones. For a particular Service Zone, administrators can enable all the authentication servers which will be used and also specify a default authentication server in the page of *Service Zone Settings*. Concurrently up to four servers can be selected and pre-configured here by administrators from the **five types** of authentication databases (LOCAL, POP3, RADIUS, LDAP, and **NTDOMAIN**). In addition, there are two servers (On-demand User and SIP) that are selected by the system. For the Authentication Settings of each Service Zone, please see ***4.1.7 Service Zones***.

Authentication Server Configuration			
Server Name	Auth Method	Postfix	Group
Server 1	LOCAL	local	Group 1
Server 2	POP3	pop3	Group 1
Server 3	RADIUS	radius	Group 1
Server 4	LDAP	ldap	Group 1
On-demand User	ONDEMAND	ondemand	Group 5
SIP	SIP	N/A	None

- **Server Name:** There are several authentication options supported by WMS-208: Server 1 to Server 4, On-demand User, and SIP. Click the hyperlink of the respective Server Name to configure the authentication server.
- **Auth Method:** There are different authentication methods in WMS-208: **LOCAL**, **POP3**, **RADIUS**, **LDAP**, **NTDOMAIN**, **ONDEMAND** and **SIP**.
- **Postfix:** A postfix represents the authentication server in a complete username. For example, **user1@local** means that this user (user1) will be authenticated against the LOCAL authentication database.

Note: *Concurrently only one server is allowed to be set as LOCAL or NTDOMAIN authentication method.*

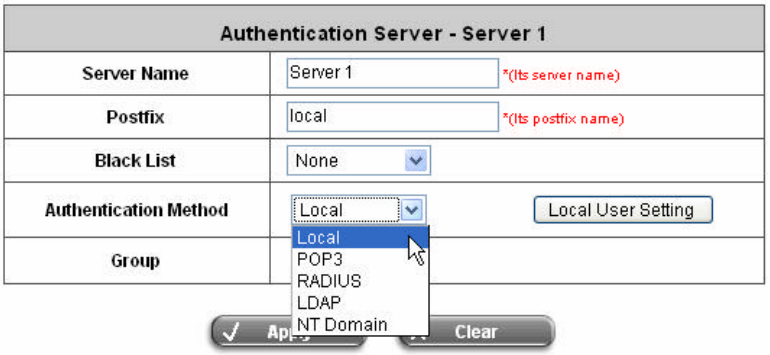
- **Group:** An authentication option, such as POP3 or NT Domain, can be set as a Group with the same QoS or Privilege Profile setting.
  For more information on Group, please refer to **Section 4.2.3. Group Configuration.**

Caution: *After clicking* ***Apply****, there will be a restart message. You must click* ***Restart*** *to apply the settings.*

- **Authentication Server Configuration**

  WMS-208 provides four authentication servers and one on-demand server that the administrator can apply with different policy. Click on the server name to set the configuration for that particular server. After completing and clicking ***Apply*** to save the settings, go back to the previous page to select a server to be the default server and enable or disable any server on the list. Users can log into the default server without the postfix to allow faster login process.

  Server 1~4: There are 5 authentication methods, **Local User, POP3, RADIUS, LDAP** and **NTDomain,** to select from.



  Server Name: Set a name for the authentication option by using numbers (0~9), alphabets (a~z or A ~Z), dash (-), underline (_), space and dot (.) only. The length of this field is up to 40 characters. This name is used for the administrator to identify the authentication options easily such as HQ-RADIUS.

  Postfix: A postfix is used to inform the system which authentication option to be used for authenticating an account (e.g. bob@BostonLdap or tim@TaipeiRadius) when multiple options are concurrently in use. One of authentication option can be assigned as default. For authentication assigned as default, the postfix can be omitted. For example, if "BostonLdap" is the postfix of the default option, Bob can login as "bob" without having to type in "bob@BostonLdap". Set a postfix that is easy to distinguish (e.g. Local) and the server numbers (0~9), alphabets (a~z or A~Z), dash (-), underline (_) and dot (.) within a maximum of 40 characters. All other characters are not allowed.

Caution: *The Policy Name cannot contain these words: MAC and IP.*

  Black List: There are 5 sets of black lists provided by the system. A user account listed in the black list is not allowed to log into the system, the client's access will be denied. The administrator may select one black list from the drop-down menu and this black list will be applied to this specific authentication option.

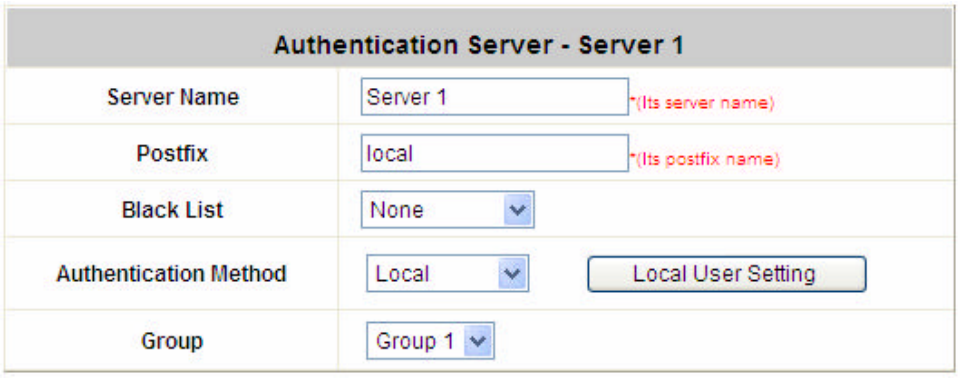
  Group: Select one Group from the drop-down list box for this specific authentication option.

  Authentication Method: Select *Local* from the drop-down list box and then click ***Local User Setting*** button to enter the **Local User Settings**. Then, click the hyperlink of ***Edit Local User List*****.**

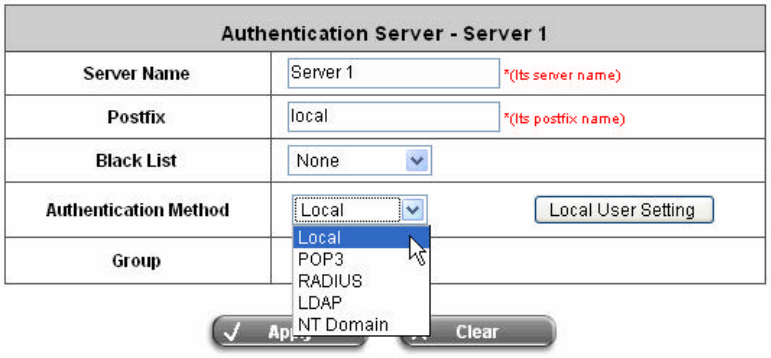
Caution: *Enabling two or more servers of the same authentication method is NOT allowed.*

4.2.1.1 Authentication Method - Local

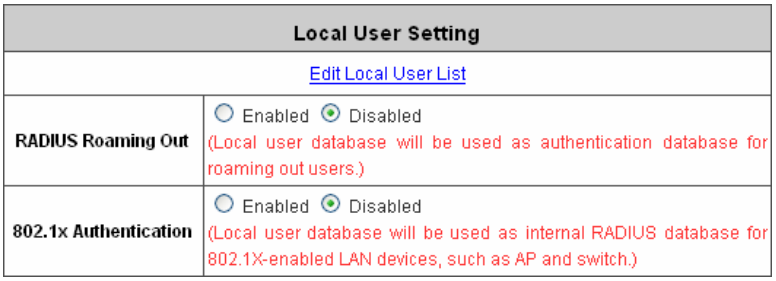
Choose **"Local User"** from the **Authentication Method** field, the button besides the pull-down menu will become **"Local User Setting"**.



Click the button of ***Local User Setting*** for further configuration.

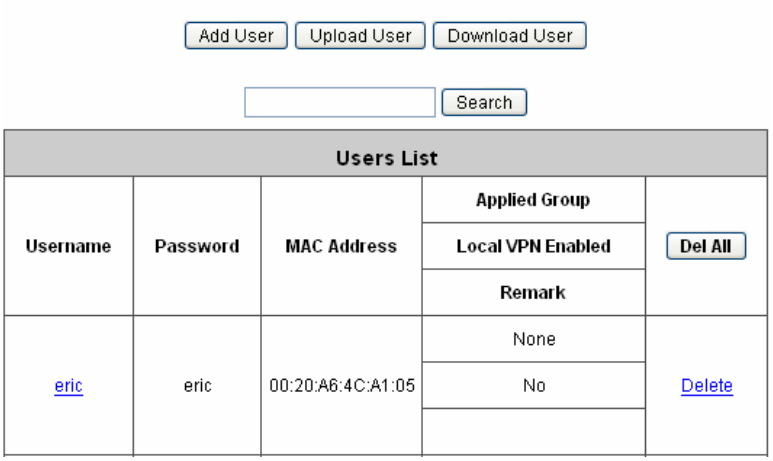


- **Edit Local User List:** It let the administrator view / add, and delete local user account. The ***Upload User*** button is for importing a list of user account from a text file. The ***Download User*** button is for exporting all local user accounts into a text file. Clicking on each user account leads to a page for configuring the individual local account. Local user account can be assigned a policy and applied Local VPN individually. Check the check box of individual local user account in the Enable Local VPN column to enable individually. MAC address of a networking device can be bound with a local user as well.


Local User Setting
Edit Local User List
RADIUS Roaming Out
Enabled
Disabled
(Local user database will be used as authentication database for roaming out users.)
802.1x Authentication
Enabled
Disabled
(Local user database will be used as internal RADIUS database for 802.1X-enabled LAN devices, such as AP and switch.)

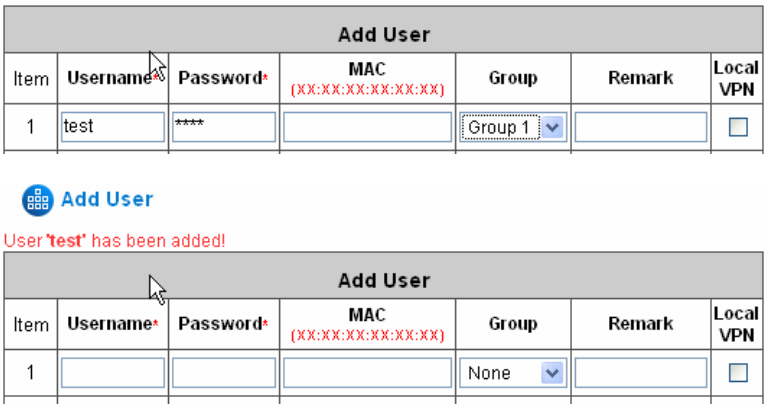
  - **Edit Local User List:** It let the administrator view, add, and delete local user account. The ***Upload User*** button is for importing a list of user account from a text file. The ***Download User*** button is for

exporting all local user accounts into a text file. Clicking on each user account leads to a page for configuring the individual local account. Local user account can be assigned a policy and applied Local VPN individually. Check the check box of individual local user account in the Enable Local VPN column to enable individually. MAC address of a networking device can be bound with a local user as well.

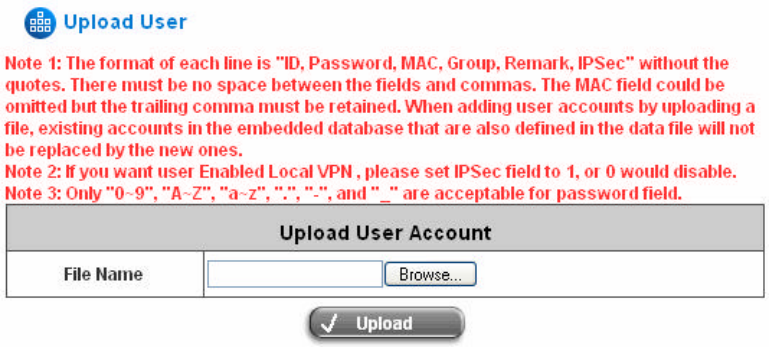


- ***Add User*:** Click this button to enter into the **Adding User(s) to the List** interface. Fill in the necessary information such as **"Username"**, **"Password"**, **"MAC"**, and **"Remark"**. Select a desired *Group* to classify local users. Check to enable *Local VPN* in the **Enable Local VPN** column. Click ***Apply*** to complete adding the user(s).

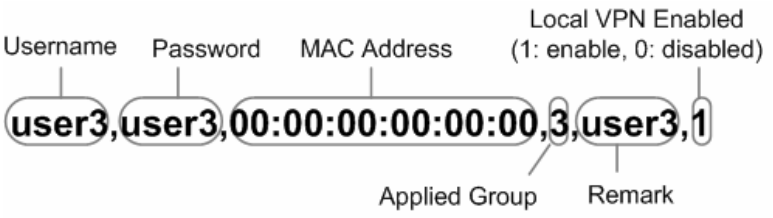
For more information on Group configuration, please refer to **Section 4.2.3. Group Configuration**.



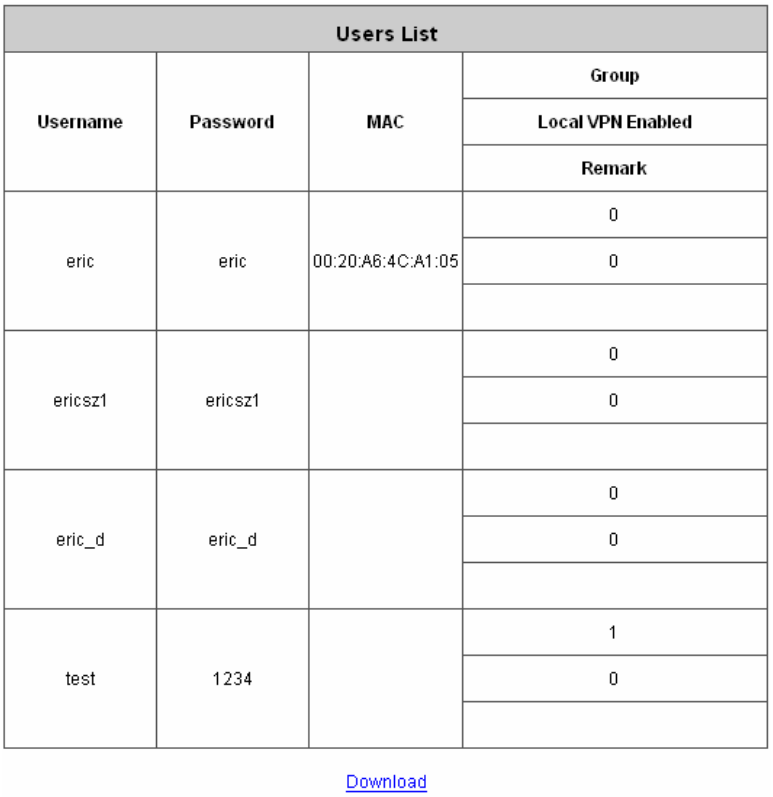
- **Upload User:** Click ***Upload User*** to enter the **Upload User from File** interface. Click the ***Browse*** button to select the text file for uploading user accounts, then click ***Upload*** to complete the upload process.


Upload User
Note 1: The format of each line is "ID, Password, MAC, Group, Remark, IPSec" without the quotes. There must be no space between the fields and commas. The MAC field could be omitted but the trailing comma must be retained. When adding user accounts by uploading a file, existing accounts in the embedded database that are also defined in the data file will not be replaced by the new ones.
Note 2: If you want user Enabled Local VPN , please set IPSec field to 1, or 0 would disable.
Note 3: Only "0~9", "A~Z", "a~z", ".", "-", and "_" are acceptable for password field.
Upload User Account
File Name
Browse...
Upload

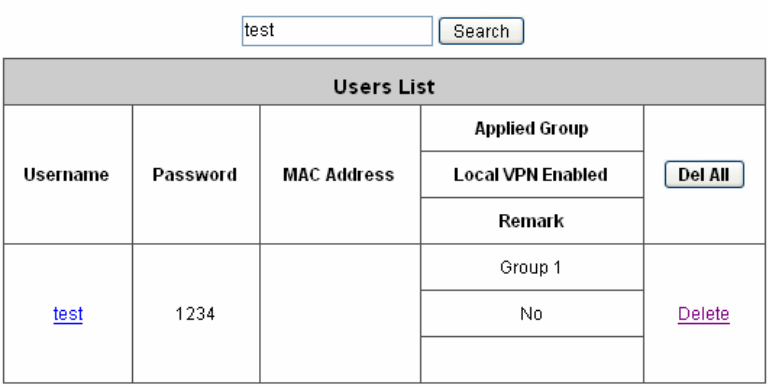
The uploading file must be a text file and each line should contain the following information in this specific order: **Username, Password, MAC Address, Applied Group, Remark,** and **Enable Local VPN**. No spaces are allowed between fields and commas. The **MAC** field can be omitted, but the trailing comma must be retained. When adding user accounts by uploading a file, the existing accounts in the embedded database will be remained but not replaced by new ones.



- ***Download User*:** Use this function to create a .txt file with all built-in user account information and then save it on disk.

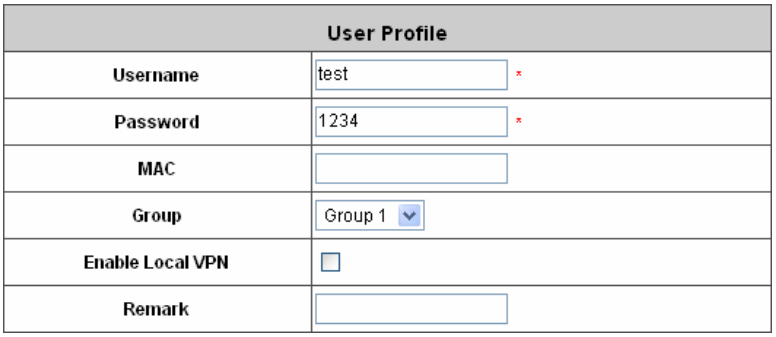


- ***Search*:** Enter a keyword of a username to be searched in the text filed and click this button to perform the search. All usernames matching the keyword will be listed.

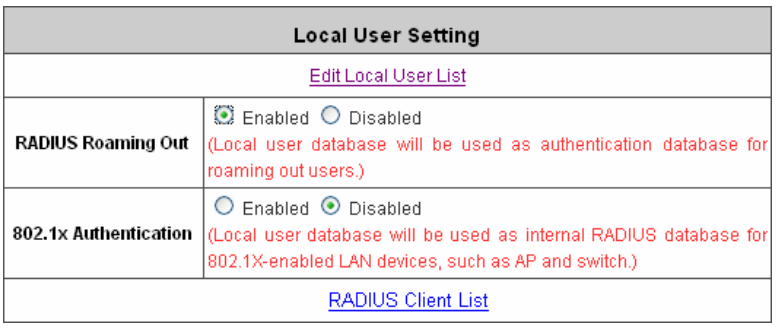


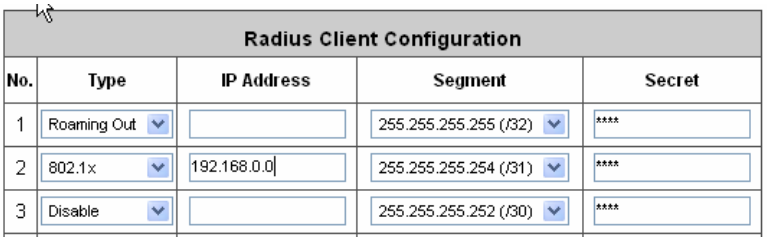
- ***Del All*:** Click on this button to delete all the users at once and click on ***Delete*** to delete the user individually.

- **Edit User:** If editing the content of individual user account is needed, click the username of the desired user account to enter the **User Profile** Interface for that particular user, and then modify or add any desired information such as *Username*, *Password*, *MAC Address* (optional), *Group* (optional), *Enable Local VPN* (optional) and *Remark* (optional). Click ***Apply*** to complete the modification.



- **Roaming Out & 802.1X Authentication:** When Account Roaming Out is enabled, the link of this function will be available to define the authorized device with IP address, Subnet Mask, and Secret Key. Please see more explanation above in the section for **Roaming Out** and the section for **802.1X Authentication**.


Local User Setting
Edit Local User List
RADIUS Roaming Out
Enabled
Disabled
(Local user database will be used as authentication database for roaming out users.)
802.1x Authentication
Enabled
Disabled
(Local user database will be used as internal RADIUS database for 802.1X-enabled LAN devices, such as AP and switch.)
RADIUS Client List

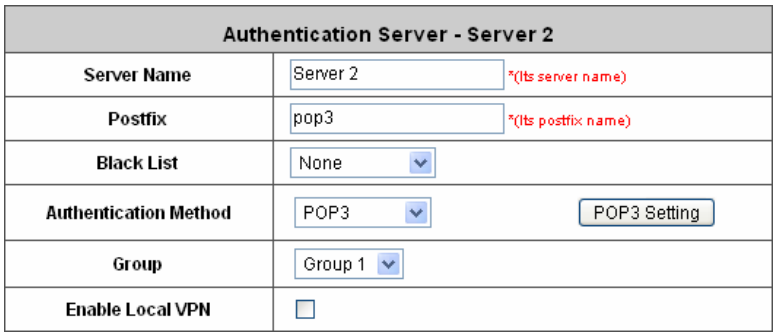


Click the hyperlink ***RADIUS Client List*** to enter the **Radius Client Configuration** interface. Choose the desired type, **Disable**, **Roaming Out** or **802.1X**, and key in the 802.1X client's IP address and network mask and then click ***Apply*** to complete the settings.

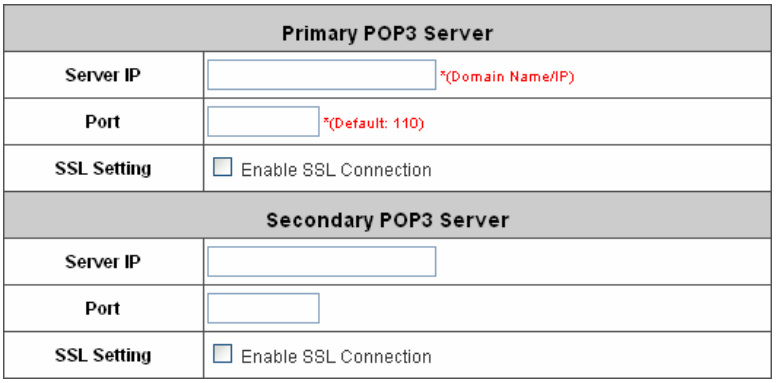
- **802.1X Authentication:** When **802.1X Authentication** is enabled, the Local authentication database will be used as a RADIUS database for connection with 802.1x enabled devices such as APs or switches.
- **Roaming Out:** The system's local user database can also be an external RADIUS database to another system. When **Account Roaming Out** is enabled, local users can login from other domains with their original local user accounts. The authentication database with their original local user accounts acts as a RADIUS Server and roaming out local users act as RADIUS clients.

4.2.1.2 Authentication Method - POP3

The system supports authentication by an external POP3 authentication server. The system is capable of supporting two POP3 servers, primary and secondary, for fault tolerance. When POP3 Authentication Database is enabled, at least one external POP3 server must be activated. The Local VPN function can be enabled for the clients authenticated by POP3 authentication method.



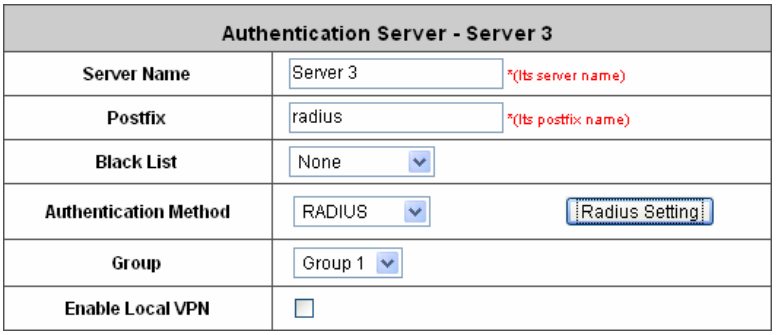
- **Name:** Set a name for the server using numbers (0~9), alphabets (a~z or A ~Z), dash (-), underline (_) and dot (.) within a maximum of 40 characters. All other characters are not allowed.
- **Postfix:** Set a postfix that is easy to distinguish (e.g. Local) for the server using numbers (0~9), alphabets (a~z or A~Z), dash (-), underline (_) and dot (.) within a maximum of 40 characters. All other characters are not allowed.
- **Black List:** There are five sets of the black lists. Select one of them or choose **"None"**. For details, please refer to **4.2.2 Black List Configuration.**
- **Group:** Select one Group from the drop-down list box for this specific authentication option.
- **Enable Local VPN:** When Local VPN function is enabled for the authentication option, upon the successful login of a client, a VPN tunnel will be established between a client's device and the system. The data passing through the VPN tunnel are encrypted. The system's Local VPN supports end-users' devices under Windows 2000 and Windows XP SP1, SP2.
- **Authentication Method:** Select *POP3* from the drop-down list box and then click ***POP3 Setting*** button for further configuration.



- **Server IP:** The IP address of the external POP3 Server.
- **Port:** The authentication port of the external POP3 Server.
- **SSL Setting**: The system supports POP3S. Check the check box beside to **Enable SSL Connection** to POP3S.

4.2.1.3 Authentication Method - RADIUS

The system supports authentication by an external RADIUS authentication server by functioning as a RADIUS authenticator for the RADIUS server. The system is capable of supporting two RADIUS servers, primary and secondary, for fault tolerance.



- **Name:** Set a name for the authentication option by using numbers (0~9), alphabets (a~z or A ~Z), dash (-), underline (_) and dot (.) within a maximum of 40 characters. All other characters are not allowed.
- **Postfix:** Set a postfix that is easy to distinguish (e.g. Radius) by using numbers (0~9), alphabets (a~z or A~Z), dash (-), underline (_) and dot (.) within a maximum of 40 characters. All other characters are not allowed.

  A postfix is used to inform the system which authentication option is used for authenticating an account (e.g. bob@BostonLdap or tim@TokyoRadius) when multiple options are concurrently in use. One of authentication options can be assigned as default. The postfix can be omitted only when the default authentication option is used. For example, if "BostonLdap" is the postfix of the default option, Bob can log in with either "bob" or "bob@BostonLdap" as his username.
- **Black List:** There are five sets of the black lists. A user account listed in the black list is not allowed to log into the system. Select one black list from the drop-down list box to be applied to this specific authentication option.
- **Group:** Select one Group from the drop-down list box for this specific authentication option.
- **Enable Local VPN:** When Local VPN function is enabled for this authentication option, upon a successful login of a client, a VPN tunnel will be established between a client's device and the system. The data passing through the VPN tunnel are encrypted. The system's Local VPN supports client devices under Windows 2000 and Windows XP SP1/SP2.
- **Authentication Method:** Select *RADIUS* from the drop-down list box and then click ***Radius Setting*** for further configuration as below. Enter the related information for the primary and/or the secondary RADIUS server (the secondary server is not required). The fields with red asterisk are required. The settings will take effect immediately after clicking ***Apply***.

Radius Setting	
802.1x Authentication	Enabled Disabled Radius Client List
Trans Full Name	Complete (e.g. user1@company.com) Only ID (e.g. user1)
NASID	
Class-Group Mapping	Edit Class-Group Mapping
Primary RADIUS Server	
Server IP	*(Domain Name/IP Address)
Authentication Port	*(Default: 1812)
Accounting Port	*(Default: 1813)
Secret Key	*
Accounting Service	Enabled Disabled
Authentication Protocol	PAP
Secondary RADIUS Server	
Server IP	(Domain Name/IP Address)
Authentication Port	
Accounting Port	
Secret Key	
Accounting Service	Enabled Disabled
Authentication Protocol	CHAP

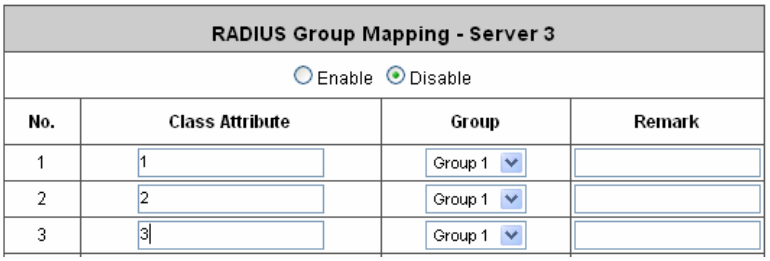
802.1X Authentication: The system supports 802.1X. When *802.1X Authentication* is enabled, the Local Authentication Database will be used as a RADIUS database for connection with 802.1X enabled devices such as access points or switches.

When the option is enabled, the hyperlink of ***Radius Client List*** will appear.

Click the hyperlink of ***Radius Client List*** to enter the ***Radius Client Configuration*** page. Choose a desired type from *Disable*, *Roaming Out* or *802.1X*. Enter the *IP Address*, Segment (*Subnet Mask),* and *Secret Key* of 802.1X clients. Click ***Apply*** to complete the settings.

Radius Client Configuration				
No.	Type	IP Address	Segment	Secret
1	Roaming Out		255.255.255.255 (/32)	****
2	802.1x	192.168.0.0	255.255.255.254 (/31)	****
3	Disable		255.255.255.252 (/30)	****

- **Trans Full Name:** When ***Complete*** option is checked, both the username and postfix will be transferred to the RADIUS server for authentication. On the other hand, when ***Only ID*** option is checked, only the username will be transferred to the external RADIUS server for authentication.
- **NASID:** The Network Access Server (NAS) Identifier of the system for the external RADIUS server.
- **Class-Group Mapping:** This function is to assign a *Group* to a RADIUS class attribute sent from the RADIUS server. When the clients classified by RADIUS class attributes log into the system via the RADIUS server, each client will be mapped to its assigned Group.

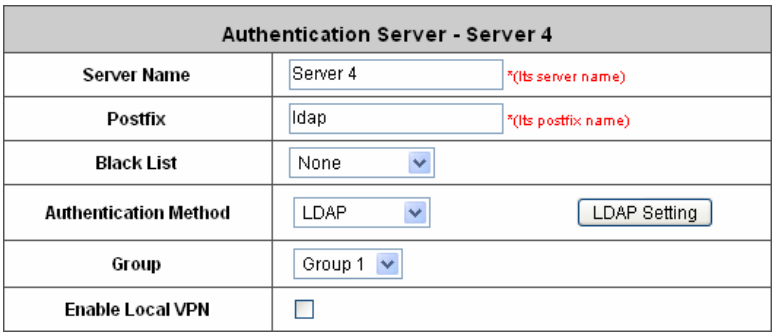


- **Server IP:** The IP address of the external RADIUS server.
- **Authentication Port:** Enter the authentication port of the RADIUS server.
- **Accounting Port:** The accounting port of the external RADIUS server.
- **Secret Key:** The Secret Key for RADIUS authentication.
- **Accounting Service:** The system supports RADIUS accounting that can be enabled or disabled.
- **Authentication Protocol:** The configuration of the system must match with that of the remote RADIUS server. **PAP** (Password Authentication Protocol) transmits passwords in plain text without encryption. **CHAP** (Challenge Handshake Authentication Protocol) is a more secure authentication protocol with hash encryption.

Notice: *If the RADIUS Server does not assign idle-timeout value, the WMS-208 will use the local idle-timeout.*

4.2.1.4 Authentication Method - LDAP

The system supports authentication by an external LDAP authentication server. The system is capable of supporting two LDAP servers, primary and secondary, for fault tolerance.



- **Server Name:** Set a name for the authentication option by using numbers (0~9), alphabets (a~z or A ~Z), dash (-), underline (_) and dot (.) within a maximum of 40 characters. All other characters are not allowed.
- **Postfix:** Set a postfix that is easy to distinguish (e.g. Ldap) by using numbers (0~9), alphabets (a~z or A~Z), dash (-), underline (_) and dot (.) within a maximum of 40 characters. All other characters are not allowed.

  A postfix is used to inform the system which authentication option is used for authenticating an account (e.g. bob@BostonLdap or tim@TokyoRadius) when multiple options are concurrently in use. One of authentication options can be assigned as default. The postfix can be omitted only when the default authentication option is used. For example, if "BostonLdap" is the postfix of the default option, Bob can log in with either "bob" or "bob@BostonLdap" as his username.
- **Black List:** There are five sets of the black lists. A user account listed in the black list is not allowed to log into the system. Select one black list from the drop-down list box to be applied to this specific authentication option.
- **Group:** Select one Group from the drop-down list box for this specific authentication option.
- **Enable Local VPN:** When Local VPN function is enabled for this authentication option, upon a successful login of a client, a VPN tunnel will be established between a client's device and the system. The data passing through the VPN tunnel are encrypted. The system's Local VPN supports client devices under Windows 2000 and Windows XP SP1/SP2.
- **Authentication Method:** Select *LDAP* from the drop-down list box and then click ***LDAP Setting*** for further configuration. Enter the related information for the primary and/or the secondary LDAP server (the secondary server is not required). The fields with red asterisk are required. The settings will take effect immediately after clicking ***Apply***.

Primary LDAP Server	
Server IP	*(Domain Name/IP)
Port	*(Ex: 389)
Base DN	*(CN=,dc=,dc=)
Account Attribute	*(Ex: uid)
Secondary LDAP Server	
Server IP	
Port	
Base DN	
Account Attribute	
Group Mapping	
Attribute-Group Mapping	Map LDAP Attributes to Group

- **Server IP:** The IP address of the external LDAP server.
- **Port:** The authentication port of the external LDAP server.
- **1Base DN:** The Distinguished Name for the navigation path of LDAP account.
- **Account Attribute**: The attribute of LDAP accounts.
- **Attribute-Group Mapping**: This function is to assign a *Group* to a LDAP attribute sent from the LDAP server. When the clients classified by LDAP attributes log into the system via the LDAP server, each client will be mapped to its assigned Group. To get and show the attribute name and value from the configured LDAP server, enter *Username* and *Password* and click ***Show Attribute***. Then, the table of attribute will be displayed. Enter the *Attribute Name* and *Attribute Value* chosen from the attribute table, and select a *Group* from the drop-down list box.

Attribute Name	Attriubute Value
CN	USER01
C	TW

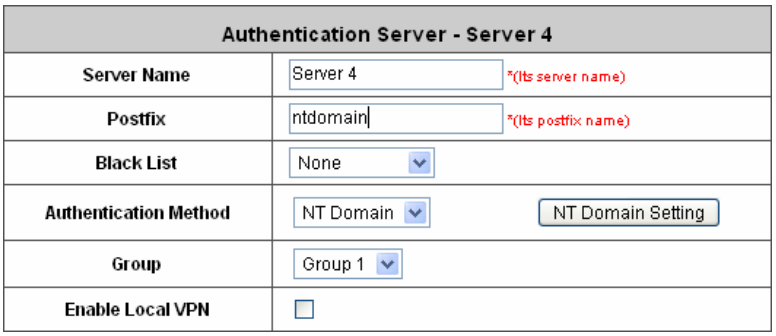
LDAP Group Mapping - Server 4

○ Enable ◉ Disable

No.	LDAP Attribute Name	LDAP Attribute Value	Group	Remark
1	CN	USER01	Group 1	
2	C	TW	Group 2	

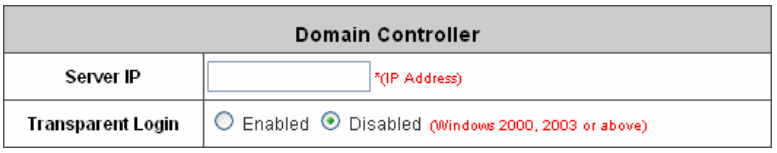
4.2.1.5 Authentication Method - NT Domain

The system supports authentication by an external NT Domain authentication database.



- **Server Name:** Set a name for the authentication option by using numbers (0~9), alphabets (a~z or A ~Z), dash (-), underline (_) and dot (.) within a maximum of 40 characters. All other characters are not allowed.
- **Postfix:** Set a postfix that is easy to distinguish (e.g. NT-Domain) by using numbers (0~9), alphabets (a~z or A~Z), dash (-), underline (_) and dot (.) within a maximum of 40 characters. All other characters are not allowed.

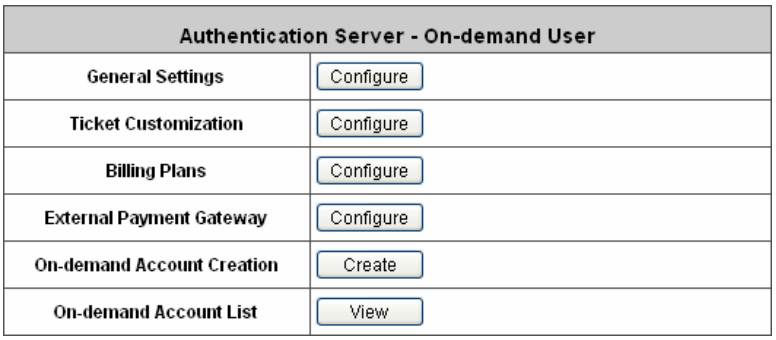
  A postfix is used to inform the system which authentication option is used for authenticating an account (e.g. bob@BostonLdap or tim@TokyoRadius) when multiple options are concurrently in use. One of authentication options can be assigned as default. The postfix can be omitted only when the default authentication option is used. For example, if "BostonLdap" is the postfix of the default option, Bob can log in with either "bob" or "bob@BostonLdap" as his username.
- **Black List:** There are five sets of the black lists. A user account listed in the black list is not allowed to log into the system. Select one black list from the drop-down list box to be applied to this specific authentication option.
- **Group:** Select one Group from the drop-down list box for this specific authentication option.
- **Enable Local VPN:** When Local VPN function is enabled for this authentication option, upon a successful login of a client, a VPN tunnel will be established between a client's device and the system. The data passing through the VPN tunnel are encrypted. The system's Local VPN supports client devices under Windows 2000 and Windows XP SP1/SP2.
- **Authentication Method:** Select *NT Domain* from the drop-down list box and click ***NT Domain Setting*** to enter the **Domain Controller** page. The settings will take effect immediately after clicking ***Apply***.



  - **Server IP:** The IP address of the external NT Domain Server.
  - **Transparent Login:** This function refers to Windows NT Domain single sign on. When *Transparent Login* is enabled, clients will log in to the system automatically after they have logged in to the NT domain, which means that clients only need to log in once.

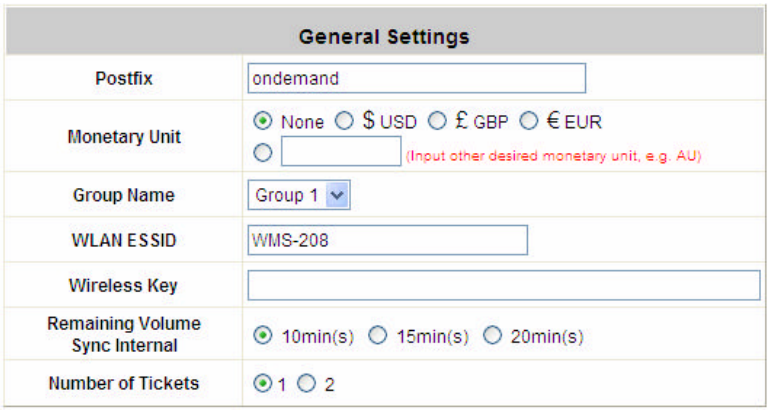
4.2.1.6 Authentication Method - ONDEMAND

There are some deployment scenarios (for example, at venues such as coffee shops, hotels, restaurants, etc.) where retail customers or casual visitors want to get wireless Internet access. To offer the Wi-Fi access (either for commercial use or for free), user accounts should be able to be created upon request and account tickets/receipts should also be provided. Therefore, **On-demand User** is designed as the authentication option for this type of deployment scenarios.



1) **General Settings**

This is the common setting for the On-demand User authentication option. The generated on-demand users and all accounts related information such as postfix and unit will be shown in this list.

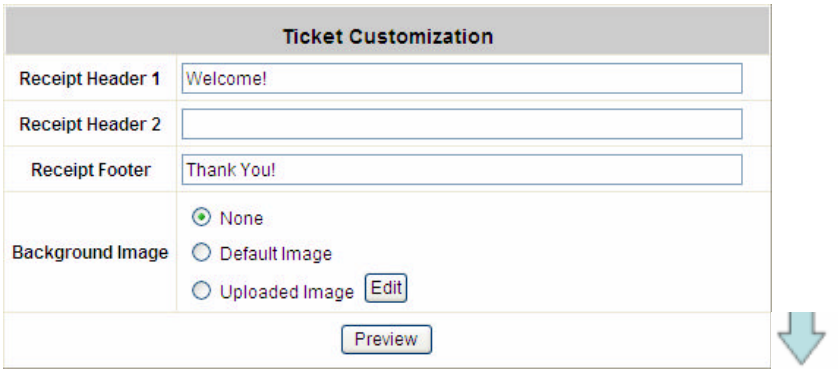


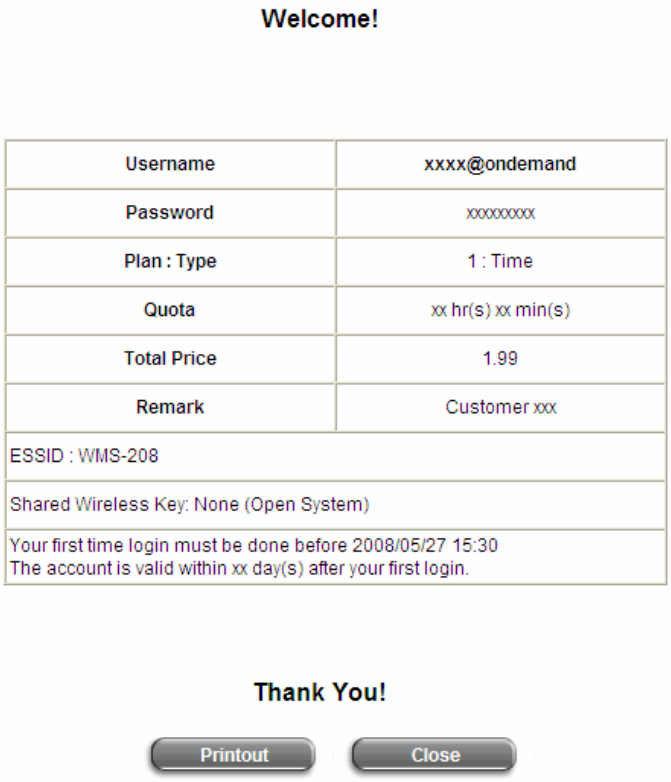
- **Postfix:** Postfix is used to inform the system which type of authentication database to be used for authentication when multiple databases are concurrently in use. Enter the postfix used for on-demand users.
- **Monetary Unit:** Select the desired monetary unit or specified the unit by users.
- **Group Name:** Select the desired group for on-demand user.
- **WLAN ESSID:** The administrator can enter the defined wireless ESSID in this field and it will be printed on the receipt for on-demand users' reference when accessing the Internet via wireless LAN service. The ESSIDs given here should be those of the Service Zones enabled for On-demand Users.
- **Wireless Key:** The administrator can enter the defined wireless key such as WEP or WPA in the field. The Wireless Key will be printed on the receipt for the on-demand users' reference when accessing the Internet via wireless LAN service.
- **Remaining Volume Sync Internal:** While the on-demand user is still logged in, the system will update the billing notice of the login successful page by the time interval defined here.

- **Number of Tickets:** Print one or duplicate receipts, when pressing the print button of the ticket printer which connected to serial port.

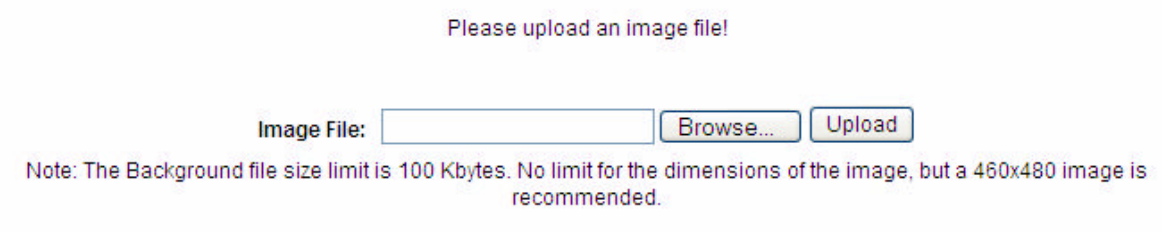
2) Ticket Customization

On-demand account ticket can be customized here and previewed on the screen.





- **Receipt Header:** There are two receipt headers supported by the system. The entered content will be printed on the receipt. These headers are optional.
- **Receipt Footer:** The entered content will be printed on the receipt. This footer is optional.
- **Background Image:** You can choose to customize the ticket by uploading your own background image for the ticket, or choose the default image or none. Click Browse to select the image file and then click upload. The background image file size limit is 100 Kbytes. No limit for the dimensions of the image is set, but a 460x480 image is recommended.


Please upload an image file!
Image File:
Browse...
Upload
Note: The Background file size limit is 100 Kbytes. No limit for the dimensions of the image, but a 460x480 image is recommended.

- **Preview:** Click ***Preview*** button, the ticket will be shown including the information of username and password with the selected background. Print the ticket here.

3) Billing Plans

Administrators can configure several billing plans. Click ***Edit*** button to enter the page of Editing Billing Plan. Click ***Apply*** to save the plan that manually set up by the administrators. Go back to the screen of Billing Plans, click ***Enable*** button, and then the plan is activated.

Billing Plans

Plan	Type	Quota	Price	Enable	Function
1	Time	2 hrs 0 mins	20	☑	Edit
2	N/A			☐	Edit
3	N/A			☐	Edit
4	N/A			☐	Edit
5	N/A			☐	Edit
6	N/A			☐	Edit
7	N/A			☐	Edit
8	N/A			☐	Edit
9	N/A			☐	Edit
0	N/A			☐	Edit

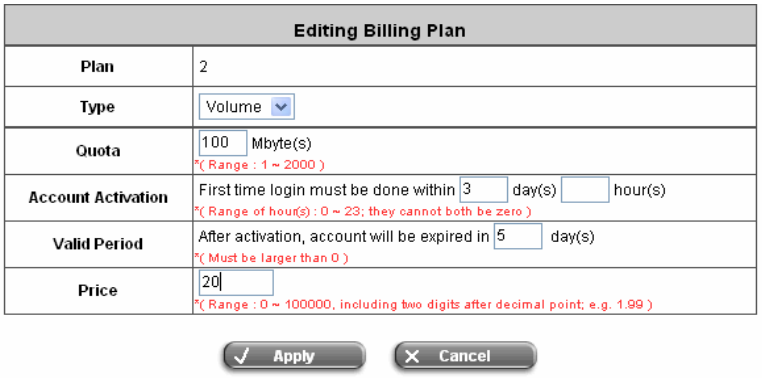
- **Plan:** The number of the specific plan.
- **Type:** This is the type of the plan, based on which it defines how the account can be used.
  - **Time:** Total period of time (xx hrs yy mins), during which On-demand users are allowed to access the network.

Editing Billing Plan

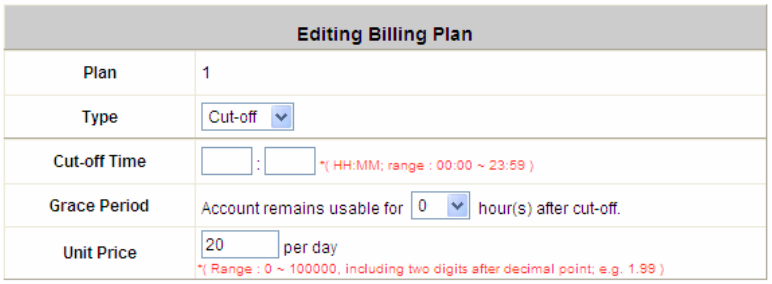
Plan	1
Type	Time
Quota	2 hr(s) 0 min(s) *(Range of min(s) : 0 ~ 59; they cannot both be zero)
Account Activation	First time login must be done within 3 day(s) 0 hour(s) *(Range of hour(s) : 0 ~ 23; they cannot both be zero)
Valid Period	After activation, account will be expired in 5 day(s) *(Must be larger than 0)
Price	20 *(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)

Apply Cancel

  - **Volume:** Total traffic volume (xx Mbytes), up to which on-demand users are allowed to transfer data.


Editing Billing Plan
Plan
2
Type
Volume
Quota
100 Mbyte(s)
*(Range : 1 ~ 2000)
Account Activation
First time login must be done within 3 day(s) hour(s)
*(Range of hour(s) : 0 ~ 23; they cannot both be zero)
Valid Period
After activation, account will be expired in 5 day(s)
*(Must be larger than 0)
Price
20
*(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)
Apply
Cancel

- **Cut-off:** Specify an absolute clock time of a day (HH:MM; range: 00:00 ~ 23:59) when the account expires.

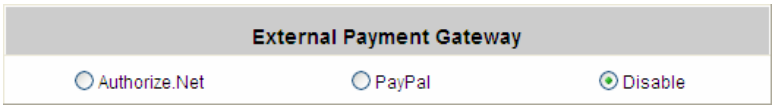

Editing Billing Plan
Plan
1
Type
Cut-off
Cut-off Time
: *(HH:MM; range : 00:00 ~ 23:59)
Grace Period
Account remains usable for 0 hour(s) after cut-off.
Unit Price
20 per day
*(Range : 0 ~ 100000, including two digits after decimal point; e.g. 1.99)

- **Quota:** The limit on how On-demand users are allowed to access the network.
- **Price:** The unit price of the plan.
- **Enable:** Click the check box to activate the plan.
- **Function:** Click the button ***Edit*** to add and edit a billing plan.

4) External Payment Gateway

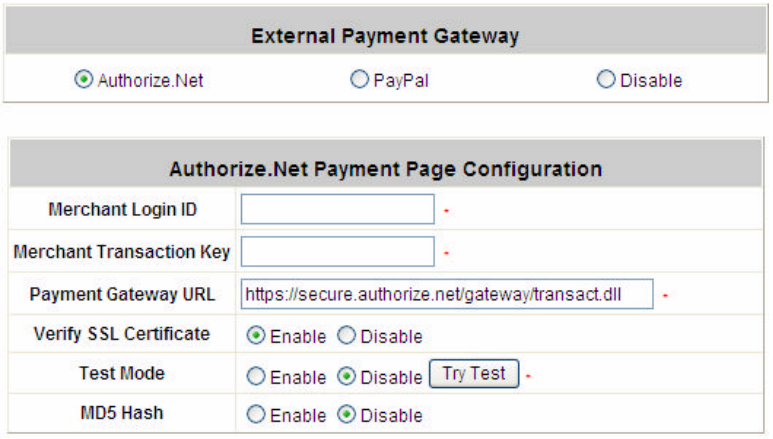
This section is for merchants to set up an external payment gateway to accept payments in order to provide wireless access service to end customers who wish to pay for the service on-line.

The three options are **Authorize.Net**, **PayPal**, and **Disable**.



- **Authorize.Net**

  Before setting up "Authorize.Net", it is required that the merchant owners have a valid Authorize.Net account. Please see ***Appendix A. Accepting Payments via Authorize.Net*** for more information about opening an Authorize.Net account, relevant maintenance functions, and an example for end users.



➢ **Authorize.Net Payment Page Configuration**

Merchant ID: This is the "Login ID" that comes with the Authorize.Net account

Merchant Transaction Key: The merchant transaction key is similar to a password and is used by Authorize.Net to authenticate transactions.

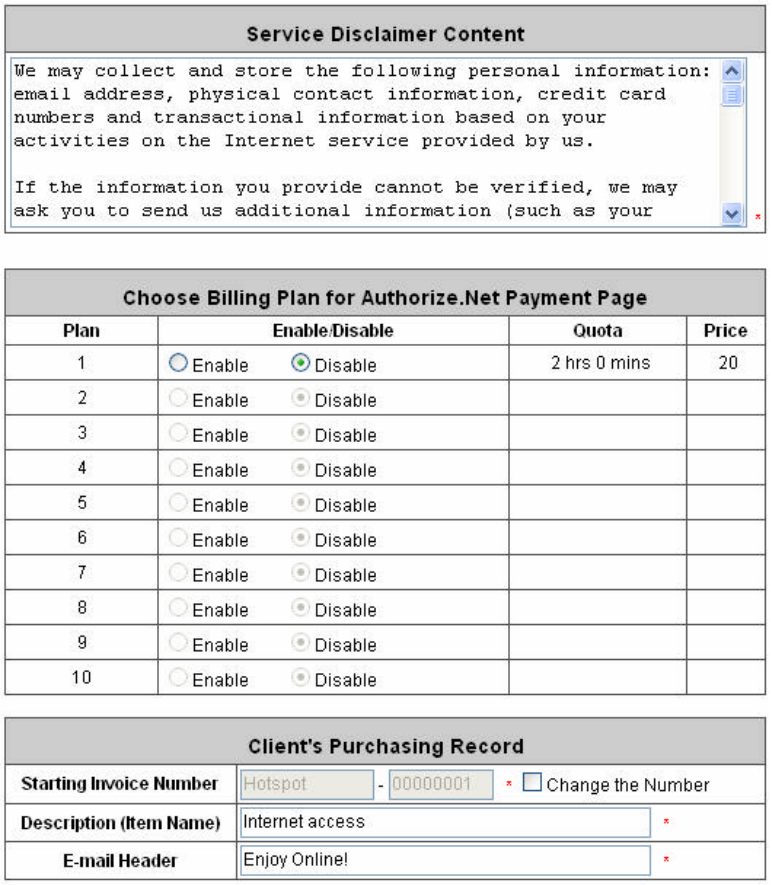
Payment Gateway URL: This is the default website address to post all transaction data.

Verify SSL Certificate: This is to help protect the system from accessing a website other than Authorize.Net

MD5 Hash: If transaction responses need to be encrypted by the Payment Gateway, enter and confirm a MD5 Hash Value and select a reactive mode. The MD5 Hash security feature enables merchants to verify that the results of a transaction, or transaction response, received by their server were actually sent from the Authorize.Net.

Test Mode: In this mode, merchants can post **test** transactions **for free** to check if the payment function works properly.

Service Disclaimer Content/ Choose Billing Plan for Authorize.Net Payment Page/Client's Purchasing Record



Service Disclaimer Content

We may collect and store the following personal information: email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.

If the information you provide cannot be verified, we may ask you to send us additional information (such as your

Choose Billing Plan for Authorize.Net Payment Page

Plan	Enable/Disable	Quota	Price
1	Enable Disable	2 hrs 0 mins	20
2	Enable Disable		
3	Enable Disable		
4	Enable Disable		
5	Enable Disable		
6	Enable Disable		
7	Enable Disable		
8	Enable Disable		
9	Enable Disable		
10	Enable Disable		

Client's Purchasing Record

Starting Invoice Number	Hotspot - 00000001 * Change the Number
Description (Item Name)	Internet access *
E-mail Header	Enjoy Online! *

➢ **Service Disclaimer Content**

View service agreements and fees for the standard payment gateway services here as well as adding new or editing services disclaimer.

➢ **Choose Billing Plan for Authorize.Net Payment Page**

These 10 plans are the plans configured in **Billing Plans** page, and all previously enabled plans can be further enabled or disabled here, as needed.

➢ **Client's Purchasing Record**

Starting Invoice Number: An invoice number may be provided as additional information with a transaction. The number will be incremented automatically for each following transaction. Click the "Change the Number" checkbox to change it.

Description (Item Name): This is the item information to describe the product (for example, Internet Access).

Email Header: Enter the information that should appear in the header of the invoice.

Authorize.Net Payment Page Fields Configuration/ Authorize.Net Payment Page Remark Content

Authorize.Net Payment Page Fields Configuration		
Item	**Displayed Text**	**Required**
☑ Credit Card Number	Credit Card Number *	☑
☑ Credit Card Expiration Date	Credit Card Expiration Date *	☑
☑ Card Type	Card Type * ☑ Visa ☑ American Express ☑ Master Card ☑ Discover	☑
☑ Card Code	Card Code *	☑
☑ E-mail	E-mail *	☐
☐ Customer ID	Room Number *	☐
☑ First Name	First Name *	☑
☑ Last Name	Last Name *	☑
☑ Company	Company *	☐
☑ Address	Address *	☐
☑ City	City *	☐
☑ State	State *	☐
☑ Zip	Zip *	☐
☑ Country	Country *	☐
☑ Phone	Phone *	☐
☑ Fax	Fax *	☐

Authorizie.Net Payment Page Remark Content
You must fill in the correct credit card number and expiration date. Card code is the last 3 digits of the security code located on the back of your credit card. If you choose to enter your e-mail address, you will receive a

- **Authorize.Net Payment Page Fields Configuration**

Item: Check the box to show this item on the customer's payment interface.

Displayed Text: Enter what needs to be shown for this field.

Required: Check the box to indicate this item as a required field.

Credit Card Number: Credit card number of the customer. The Payment Gateway will only accept card numbers that correspond to the listed card types.

Credit Card Expiration Date: Month and year expiration date of the credit card. This should be entered in the format of MMYY. For example, an expiration date of July September 2009 should be entered as 0709.

Card Type: This value indicates the level of match between the Card Code entered on a transaction and the value that is on file with a customer's credit card company. A code and narrative description are provided indicating the results returned by the processor.

Card Code: The three- or four-digit code assigned to a customer' s credit card number (found either on the front of the card at the end of the credit card number or on the back of the card).

E-mail: An email address may be provided along with the billing information of a transaction. This is the customer's email address and should contain an @ symbol.

Customer ID: This is an internal identifier for a customer that may be associated with the billing

information of a transaction. This field may contain any format of information.

First Name: The first name of a customer associated with the billing or shipping address of a transaction. In the case when John Doe places an order, enter John in the First Name field indicating this customer's name.

Last Name: The last name of a customer associated with the billing or shipping address of a transaction. In the case when John Doe places an order, enter Doe in the Last Name field indicating this customer's name.

Company: The name of the company associated with the billing or shipping information entered on a given transaction.

Address: The address entered either in the billing or shipping information of a given transaction.

City: The city is associated with either the billing address or shipping address of a transaction.

State: A state is associated with both the billing and shipping address of a transaction. This may be entered as either a two-character abbreviation or the full text name of the state.

Zip: The ZIP code represents the five or nine digit postal code associated with the billing or shipping address of a transaction. This may be entered as five digits, nine digits, or five digits and four digits.

Country: The country is associated with both the billing and shipping address of a transaction. This may be entered as either an abbreviation or full value.

Phone: A phone number is associated with both a billing and shipping address of a transaction. Phone number information may be entered as all number or it may include parentheses or dashes to separate the area code and number.

Fax: A fax number may be associated with the billing information of a transaction. This number may be entered as all number or contain parentheses and dashes to separate the area code and number.

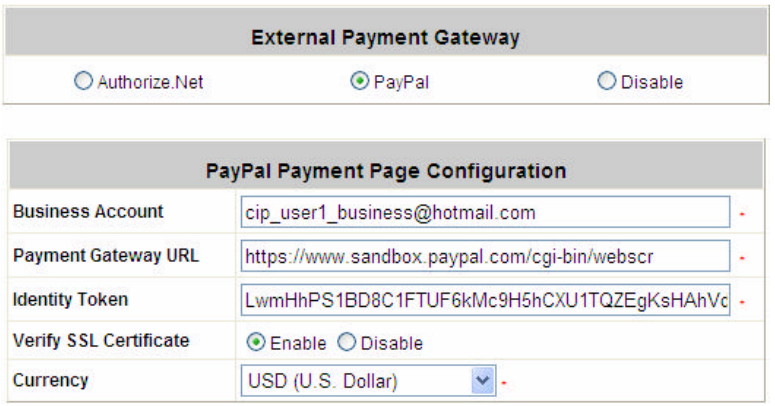
- **Authorizie.Net Payment Page Remark Content**

Enter additional details for the transaction such as Tax, Freight and Duty Amounts, Tax Exempt status, and a Purchase Order Number, if applicable.

- **PayPal**

Before setting up "PayPal", it is required that the merchant owners have a valid PayPal "Business Account". Please see ***Appendix B. Accepting Payments via PayPal*** for more information about setting up a PayPal Business Account, relevant maintenance functions, and an example for end users.

After opening a PayPal Business Account, the merchant should find the **"Identity Token"** of this PayPal account to continue **"PayPal Payment Page Configuration"**.



➢ **PayPal Payment Page Configuration**

Business Account: This is the "Login ID" (email address) that is associated with the PayPal Business Account.

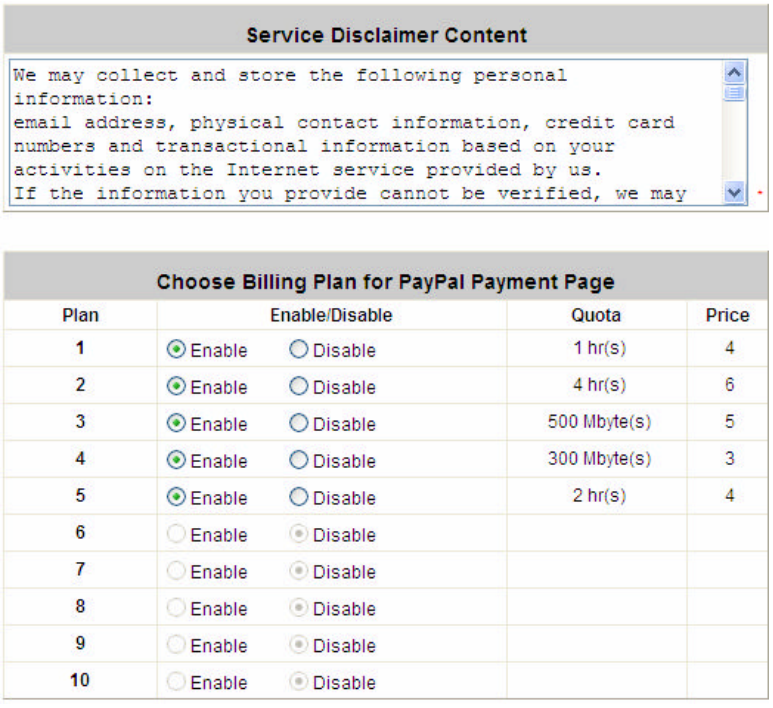
Payment Gateway URL: This is the default website address to post all transaction data.

Identity Token: This is the key used by PayPal to validate all the transactions.

Verify SSL Certificate: This is to help protect the system from accessing a website other than PayPal

Currency: It is the currency to be used for the payment transactions.

Service Disclaimer Content /Choose Billing for Payment Page


Service Disclaimer Content
We may collect and store the following personal information:
email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.
If the information you provide cannot be verified, we may
Choose Billing Plan for PayPal Payment Page
Plan
Enable/Disable
Quota
Price
1 Enable Disable 1 hr(s) 4
2 Enable Disable 4 hr(s) 6
3 Enable Disable 500 Mbyte(s) 5
4 Enable Disable 300 Mbyte(s) 3
5 Enable Disable 2 hr(s) 4
6 Enable Disable
7 Enable Disable
8 Enable Disable
9 Enable Disable
10 Enable Disable

➢ **Service Disclaimer Content**

View service agreements and fees for the standard payment gateway services here as well as adding new or editing services disclaimer.

➢ **Choose Billing Plan for PayPal Payment Page**

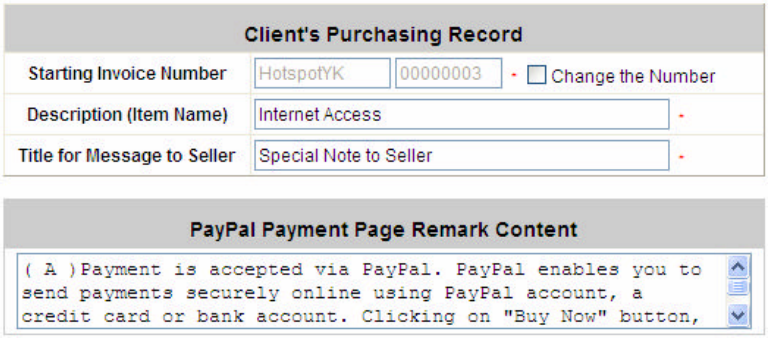
These 10 plans are the plans configured in **Billing Plans** page, and all previously enabled plans can be further enabled or disabled here, as needed.

Enable/Disable: Choose to enable or disable the plan.

Quota: The usage time or condition of each plan.

Price: The price charged for this plan.

Client's Purchasing Record/ PayPal Payment Page Remark Content


Client's Purchasing Record
Starting Invoice Number
HotspotYK
00000003
Change the Number
Description (Item Name)
Internet Access
Title for Message to Seller
Special Note to Seller
PayPal Payment Page Remark Content
(A)Payment is accepted via PayPal. PayPal enables you to send payments securely online using PayPal account, a credit card or bank account. Clicking on "Buy Now" button,

➢ **Client's Purchasing Record**

Starting Invoice Number: An invoice number may be provided as additional information with a transaction. The number will be incremented automatically for each following transaction. Click the "Change the Number" checkbox to change it.

Description (Item Name): This is the item information to describe the product (for example, Internet Access).

Title for Message to Seller: Administrators can edit the header "**title**" of the message note, used in the PayPal payment page.

➢ **PayPal Payment Page Remark Content**

The message content will be displayed as a special notice to end customers in the page of "Rate Plan". For example, it can describe the cautions for making a payment via PayPal.

5) On-demand Account Creation

On-demand accounts are listed and related. When at least one plan is enabled, the administrator can generate on-demand user accounts here. Click this to enter the On-demand Account Creation screen. Click on the ***Create*** button of the desired plan and an on-demand user account will be created. Click ***Print*** to print a receipt which will contain the on-demand user's information, including the username and password.

Note: *If no Billing plan is enabled, accounts cannot be created by clicking Create button. Please goes back to Billing Plans to active at least one Billing plan by clicking Edit button and Apply the setting to activate the plan.*
The printer used by Print is a pre-configured printer connected to the administrator's computer.

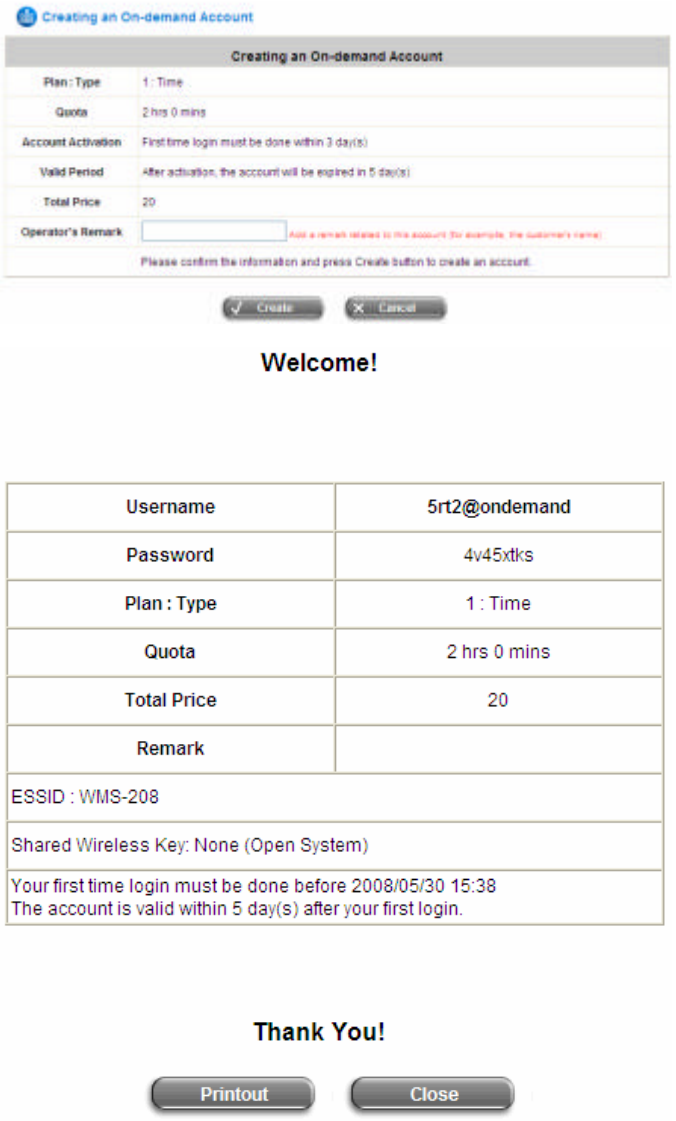
On-demand Account Creation

Plan	Type	Quota	Price ($)	Status	Function
1	Time	1 hr(s) 2 min(s)	2	Enabled	Create
2	Time	12 hr(s)	3.99	Enabled	Create
3	Volume	500 Mbyte(s)	5	Enabled	Create
4	N/A	N/A	N/A	Disabled	Create
5	N/A	N/A	N/A	Disabled	Create
6	N/A	N/A	N/A	Disabled	Create
7	N/A	N/A	N/A	Disabled	Create
8	N/A	N/A	N/A	Disabled	Create
9	N/A	N/A	N/A	Disabled	Create
0	N/A	N/A	N/A	Disabled	Create

- **Plan:** The number of a specific plan.
- **Type:** Show one type of the plan in Time, Volume or Cut-off.
- **Quota:** The Time Volume is how long the on-demand user is allowed to access the Internet.
- **Price:** The unit price of each plan.
- **Status:** Show the status in enabled or disabled.
- **Function:** Press ***Create*** button for the desired plan. You can add an operator's remark and press the **Create** button again. An On-demand user account will be created, and then click ***Printout*** to print a receipt which will contain this on-demand user's information.

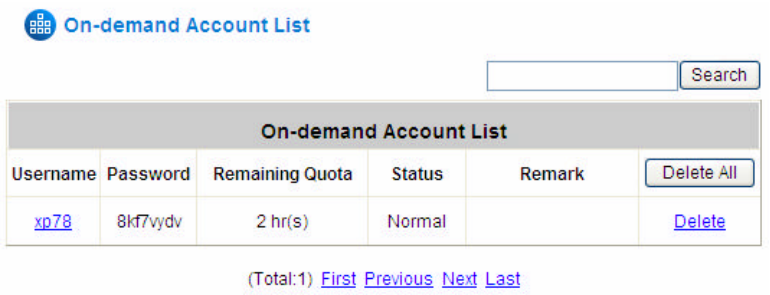
On-demand Account Creation

Plan	Type	Quota	Price ($)	Status	Function
1	Time	1 hr(s) 2 min(s)	2	Enabled	Create
2	Time	12 hr(s)	3.99	Enabled	Create
3	Volume	500 Mbyte(s)	5	Enabled	Create



6) On-demand Account List

All created On-demand accounts are listed and related information on is also provided.

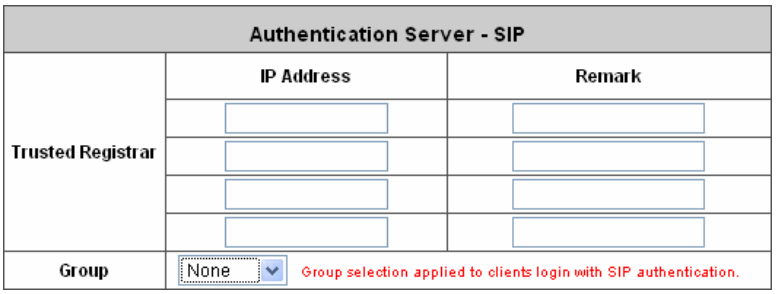


- **Search:** Enter a keyword of a username to be searched in the text filed and click this button to perform the search. All usernames matching the keyword will be listed.
- **Username:** The login name of the user.
- **Password:** The login password of the user.
- **Remaining Quota:** The remaining time or volume that the user can continue to use to access the network.

- **Status:** The status of the account.
  - **Normal:** the account is not currently in use and also does not exceed the quota limit.
  - **Online:** the account is currently in use.
  - **Expired:** the account is not valid any more, even there is remaining quota to be used.
  - **Out of Quota:** the account has exceeded the quota limit
  - **Redeemed:** the account has been applied for account renewal.
- **Remark:** The remark added by the operator at the time of ticket creation.
- **Delete All:** This will delete all the users at once.
- **Delete:** This will delete the users individually.

4.2.1.7 Authentication Method - SIP

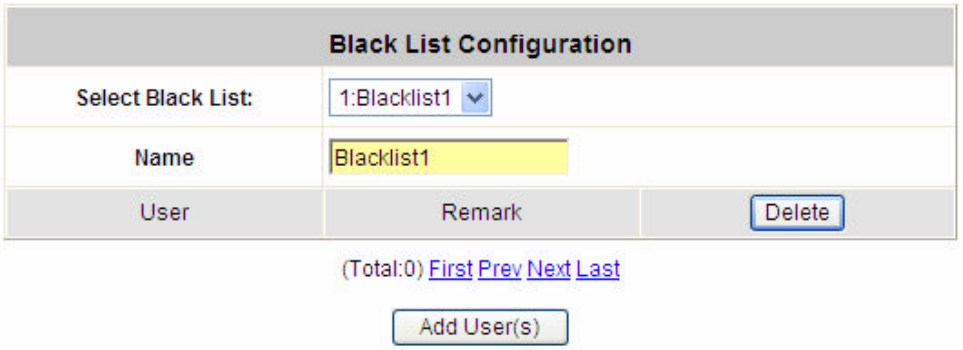
The system provides SIP proxy for SIP clients (devices or soft clients) pass through NAT. After enable SIP proxy server, all SIP traffic can pass through NAT with a selective but fixed WAN interface. Administrator will be able to add trusted SIP Registrars up to four of them. A group can be chosen to govern SIP traffic.



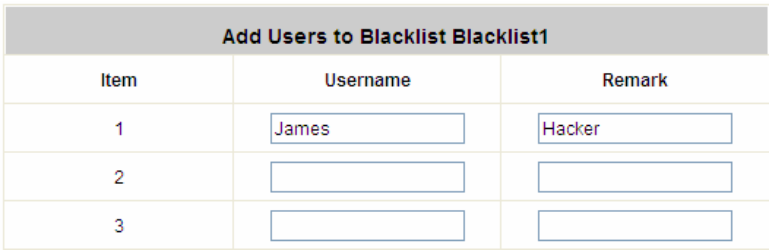
- **SIP:** SIP authentication supports 4 Trusted SIP Registrar.
- **IP Address:** The IP address of the Trusted SIP Registrar.
- **Remark:** The administrator can enter extra information in this field for remark.
- **Group:** A Group option can be applied to the clients who login with SIP Authentication. Be noted that the specific route of the applied Policy for the selected Group cannot conflict with the assigned WAN interface for SIP authentication.

4.2.2 Black List Configuration

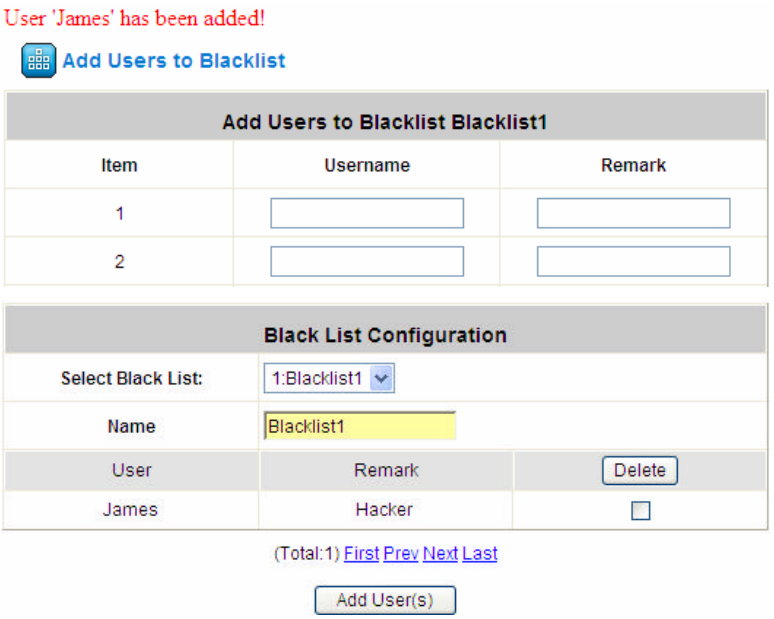
The administrator can add, delete, or edit the black list for user access control. Each black list can include up to 40 users. Users' accounts that appear in the black list will be denied of network access. The administrator can use the pull-down menu to select the desired black list.



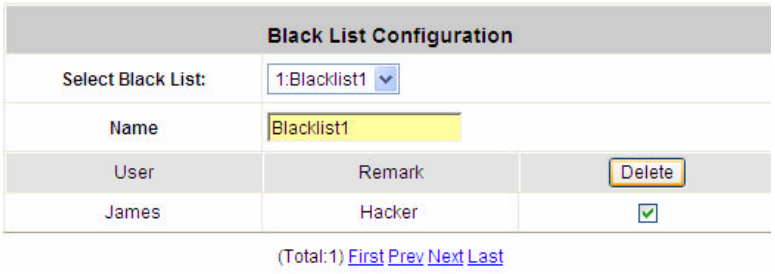
- **Select Black List:** There are 5 lists to select from for the desired black list.
- **Name:** Set the black list name and it will show on the drop down box above.
- **Add User to List:** Click the hyperlink to add users to the selected black list.



After entering the usernames in the **"Username"** blanks and the related information in the **"Remark"** blank (not required), click ***Apply*** to add the users.

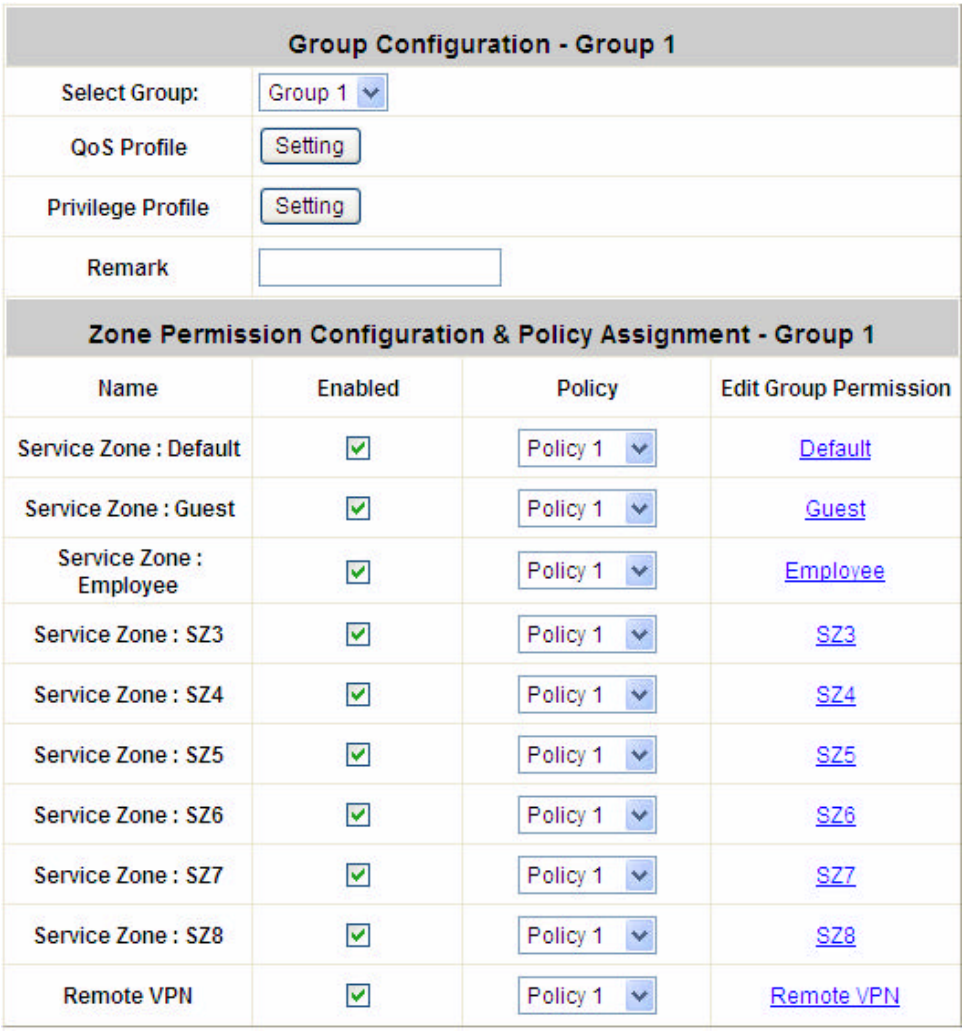


If removing a user from the black list is desired, select the user's **"Delete"** check box and then click the ***Delete*** button to remove that user from the black list.



4.2.3 Group Configuration

There are 8 groups to choose from. Local users can be classified by applying Group options. A Group which is allowed to access a Service Zone can be applied with a Policy within this zone. The same Group within different Service Zones can be applied with different Policies as well as different Authentication Options.



Group Configuration - Group 1			
Select Group:	Group 1		
QoS Profile	Setting		
Privilege Profile	Setting		
Remark			
Zone Permission Configuration & Policy Assignment - Group 1			
Name	Enabled	Policy	Edit Group Permission
Service Zone : Default	☑	Policy 1	Default
Service Zone : Guest	☑	Policy 1	Guest
Service Zone : Employee	☑	Policy 1	Employee
Service Zone : SZ3	☑	Policy 1	SZ3
Service Zone : SZ4	☑	Policy 1	SZ4
Service Zone : SZ5	☑	Policy 1	SZ5
Service Zone : SZ6	☑	Policy 1	SZ6
Service Zone : SZ7	☑	Policy 1	SZ7
Service Zone : SZ8	☑	Policy 1	SZ8
Remote VPN	☑	Policy 1	Remote VPN

- **Group Configuration – Group 1**
  - **QoS Profile:** Set parameters for traffic classification.

Group 1 - Traffic Configuration	
Traffic Class	Best Effort
Group Total Downlink	Unlimited
Individual Maximum Downlink	Unlimited
Individual Request Downlink	None
Group Total Uplink	Unlimited
Individual Maximum Uplink	Unlimited
Individual Request Uplink	None

- **Traffic Class:** A Traffic Class can be chosen for a Group of users. There are four traffic classes: ***Voice***, ***Video***, ***Best-Effort*** **and** ***Background***. Voice and Video traffic will be placed in the high priority queue. When Best-Effort or Background is selected, more bandwidth management options such as Downlink and Uplink Bandwidth will appear.
- **Group Total Downlink:** Defines the maximum bandwidth allowed to be shared by clients within this Group.
- **Individual Maximum Downlink:** Defines the maximum downlink bandwidth allowed for an individual client belonging to this Group. The Individual Maximum Downlink cannot exceed the value of Group Total Downlink.
- **Individual Request Downlink:** Defines the guaranteed minimum downlink bandwidth allowed for an individual client belonging to this Group. The Individual Request Downlink cannot exceed the value of Group Total Downlink and Individual Maximum Downlink.
- **Group Total Uplink:** Defines the maximum uplink bandwidth allowed to be shared by clients within this Group.
- **Individual Maximum Uplink:** Defines the maximum uplink bandwidth allowed for an individual client belonging to this Group. The Individual Maximum Uplink cannot exceed the value of Group Total Uplink.
- **Individual Request Uplink:** Defines the guaranteed minimum bandwidth allowed for an individual client belonging to this Group. The Individual Request Uplink cannot exceed the value of Group Total Uplink and Individual Maximum Uplink.

➢ **Privilege Profile:**

Group 1 - Privilege Configuration	
Change Password Privilege	○ Enable ◉ Disable

- **Change Password Privilege:** When *Change Password Privilege* is enabled, the authenticated local users within this Group are allowed to change their password via the Login Success Page.

- **Zone Permission Configuration & Policy Assignment – Group X**

  A Group can be assigned to one Service Zone or multiple Service Zones. Moreover, a Group can be applied with different Policies within different Service Zones. Remote VPN is considered as a zone, where clients log into the system via remote VPN.

Group Configuration - Group 1			
Select Group:	Group 1		
QoS Profile	Setting		
Privilege Profile	Setting		
Remark			
Zone Permission Configuration & Policy Assignment - Group 1			
Name	**Enabled**	**Policy**	**Edit Group Permission**
Service Zone : Default	☑	Policy 1	Default
Service Zone : SZ1	☑	Policy 1	SZ1
Service Zone : SZ2	☑	Policy 1	SZ2
Service Zone : SZ3	☑	Policy 1	SZ3
Service Zone : SZ4	☑	Policy 1	SZ4
Service Zone : SZ5	☑	Policy 1	SZ5
Service Zone : SZ6	☑	Policy 1	SZ6
Service Zone : SZ7	☑	Policy 1	SZ7
Service Zone : SZ8	☑	Policy 1	SZ8
Remote VPN	☑	Policy 1	Remote VPN

  - **Name:** The name of Service Zones and Remote VPN.
  - **Enabled:** Select *Enabled* to allow clients of this Group to log into the selected Service Zones. For example, the above figure shows that users in Group 1 can access network services via every Service Zone as well as Remote VPN under constraints of Policy 1.
  - **Policy:** Select a *Policy* that the Group will be applied with when accessing respective Service Zones.
  - **Edit Group Permission:** The relation between Group and Service Zone is many to many; every Group can access network services via more than one Service Zone, and meanwhile, each Service Zone can serve more than one Group.

  Click the hyperlink in the **Edit Group Permission** column to enter the **Group Configuration** interface, which is based on the role of Service Zone, to configure the relation between Group and Zone.

Group Permission - Service Zone : Default			
Group Option	Enabled	Policy	Edit Group Option
Group 1	☑	Policy 1	Group 1
Group 2	☑	Policy 2	Group 2
Group 3	☑	Policy 3	Group 3
Group 4	☑	Policy 4	Group 4
Group 5	☑	Policy 5	Group 5
Group 6	☑	Policy 6	Group 6
Group 7	☑	Policy 7	Group 7
Group 8	☑	Policy 8	Group 8

- **Group Option:** The name of Group options available for selection.
- **Enabled:** Select *Enabled* to allow clients of the enabled Groups to log in to this Service Zone under constraints of the selected Policies.

  Check ***Enabled*** of the respected Group to assign it/them to the Service Zone listed. For example, the above figure shows, clients in Group 1~8 can access Default Service Zone, where they are governed by Policy 1~8 respectively.
- **Policy:** Select a *Policy* that the Group will be applied with when accessing this Service Zone.
- **Edit Group Option:** Click the hyperlink in the **Edit Group Option** column to enter **Zone Permission Configuration & Policy Assignment** interface, which is based on the role of Group, to configure the relation between Group and Zone.

4.2.4 Policy Configuration

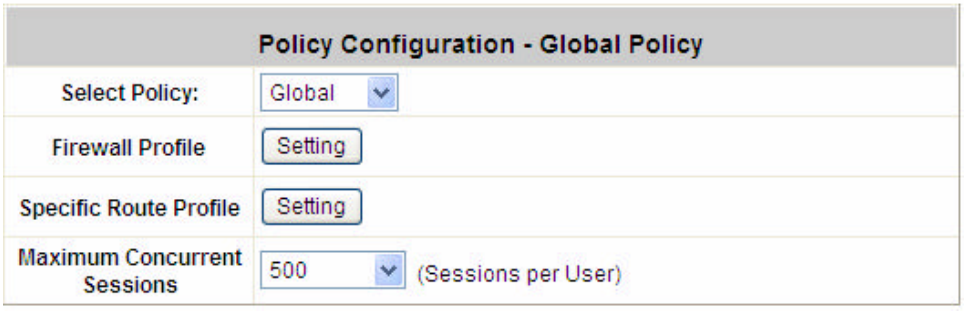
WMS-208 supports multiple Policies, including one **Global Policy** and 12 individual **Policy**. Each Policy consists of access control profiles that can be configured respectively and applied to a certain Group of users. **Global Policy** is the system's universal policy and applied to all clients, while other individual Policy can be selected and defined to be applied to any Service Zone.

The clients belonging to a Service Zone will be bound by an applied Policy. In addition, a Policy can be applied at a Group basis; a Group of users can be bound by a Policy. The same Group can be applied with different Policies within different Service Zones.

When the type of authentication database is RADIUS, the **Class-Group Mapping** function will be available to allow the administrator to assign a Group for a RADIUS class attribute; therefore, a Policy applied to this Group will be mapped to a user Group of a RADIUS class attribute. When the type of authentication database is LDAP, the **Attribute-Group Mapping** function will be available to allow administrator to assign a Group for LDAP Attribute; therefore, a Policy applied to this Group will be mapped to a user Group of a LDAP attribute. When the type of database is SIP, the **Group** selection function will be available to allow administrator to assign a Group option for all SIP clients.

4.2.4.1 Global Policy

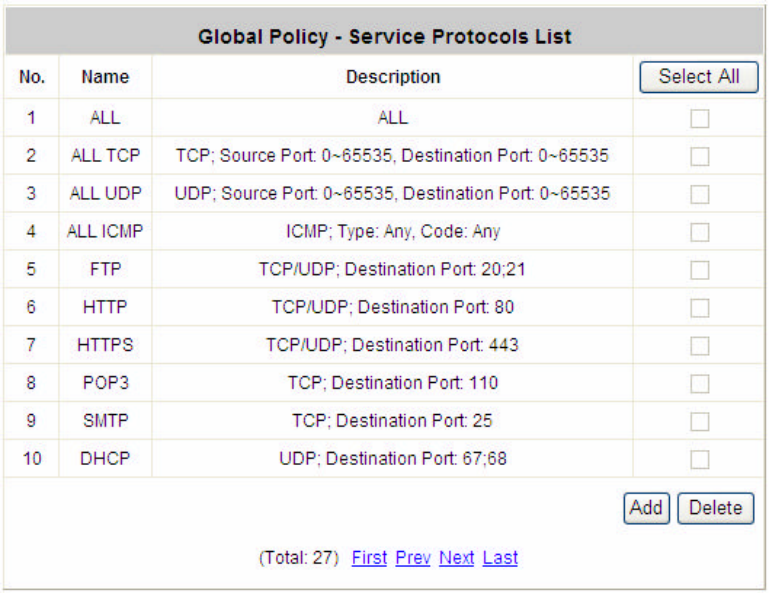
Global is the system's universal policy including **Firewall Rules**, **Specific Routes Profile** and **Maximum Concurrent Session** which will be applied to all users unless the user has been regulated and applied to another policy.



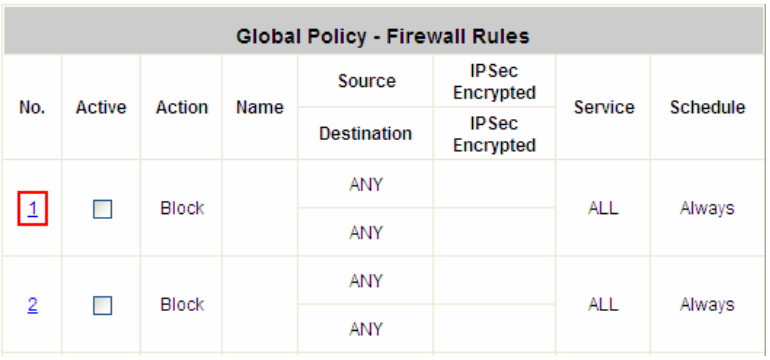
- **Select Policy:** Select **Global** to set the **Firewall Profile**, **Specific Route Profile** and **Privilege Profile**.
- **Firewall Profile:** Global policy and each policy have a firewall service list and a set of firewall profile which is composed of firewall rules.
- **Specific Route Profile:** The default gateway of WAN1, WAN2, or a desired IP address can be defined in a policy. When Specific Default Route is enabled, all clients applied this policy will access the Internet through this default gateway.
- **Maximum Concurrent Sessions:** Set the maximum concurrent sessions for each client.

- **Firewall Profile:** Click ***Setting*** for **Firewall Profile**. The Firewall Configuration will appear. Click **Predefined and Custom Service Protocols** to edit the protocol list. Click **Firewall Rules** to edit the rules.

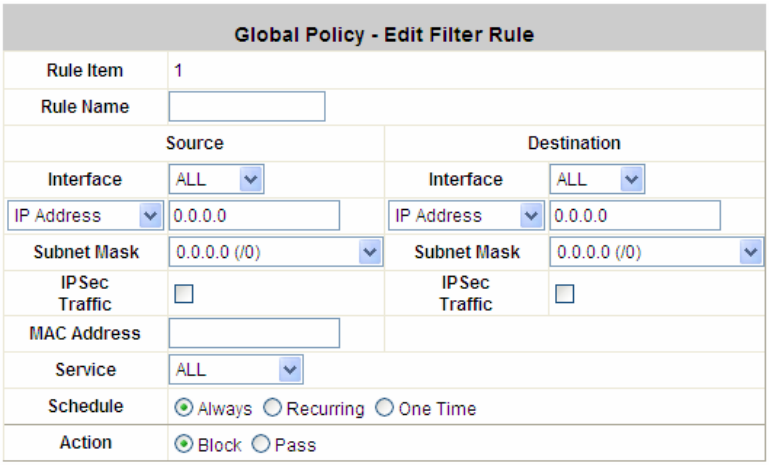
  - **Predefined and Custom Service Protocols:** There are predefined service protocols available for firewall rules editing. The administrator is able to add new custom service protocols by clicking ***Add***, and delete the added protocols with ***Select All*** and ***Delete*** operations.
    This link leads to a Service Protocols List where the administrator can defined a list of service by protocols (TCP/UDP/ICMP/IP).


Global Policy - Service Protocols List
No. Name Description Select All
1 ALL ALL
2 ALL TCP TCP; Source Port: 0~65535, Destination Port: 0~65535
3 ALL UDP UDP; Source Port: 0~65535, Destination Port: 0~65535
4 ALL ICMP ICMP; Type: Any, Code: Any
5 FTP TCP/UDP; Destination Port: 20;21
6 HTTP TCP/UDP; Destination Port: 80
7 HTTPS TCP/UDP; Destination Port: 443
8 POP3 TCP; Destination Port: 110
9 SMTP TCP; Destination Port: 25
10 DHCP UDP; Destination Port: 67;68
Add Delete
(Total: 27) First Prev Next Last

  - **Firewall Rules:** Click the number of ***Filter Rule No.*** to edit individual rules and click ***Apply*** to save the settings. The rule status will show on the list. Check **"Active"** box and click ***Apply*** to enable that rule.
    This link leads to the Firewall Rules page. Rule No.1 has the highest priority; Rule No.2 has the second priority and so on. Each firewall rule is defined by Source, Destination and Pass/Block action. Optionally, a Firewall Rule Schedule can be set to specify when the firewall rule is enforced. It can be set to Always, Recurring or One Time.

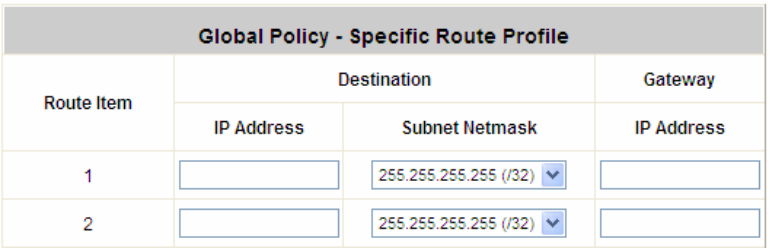

Global Policy - Firewall Rules
No. Active Action Name Source IPSec Encrypted Service Schedule
Destination IPSec Encrypted
1 Block ANY ALL Always
ANY
2 Block ANY ALL Always
ANY

Selecting the Filter Rule Number 1 as an example:



- **Rule Number:** This is the rule selected "1". Rule No. 1 has the highest priority; rule No. 2 has the second priority, and so on.
- **Rule Name:** The rule name can be changed here.
- **Source/Destination – Interface/Zone:** There are choices of **ALL, WAN1**, **WAN2**, **Default**, and the named **Service Zones** to be applied for the traffic interface.
- **Source/Destination – IP Address/Domain Name:** Enter the source and destination IP addresses. Domain Host filtering is supported but Domain name filtering is not.
- **Source/Destination – Subnet Mask:** Select the source and destination subnet masks.
- **Source- MAC Address:** The MAC Address of the source IP address. This is for specific MAC address filter.
- **Source/Destination – IPSec Encrypted:** Check the box for only filtering on the encrypted traffic.
- **Service Protocol:** There are defined protocols in the **service protocols list** to be selected.
- **Schedule:** When schedule is selected, clients assigned with this policy are applied the firewall rule only within the time checked. There are three options, **Always**, **Recurring** and **One Time. Recurring** is set with the hours within a week.
- **Action for Matched Packets:** There are two options, **Block** and **Pass**. **Block** is to prevent packets from passing and **Pass** is to permit packets passing.

➢ **Specific Route Profile:** Click the button of ***Setting*** for **Specific Route Profile**, the Specific Route Profile list will appear.



- **Route No.:** The number of route.
- **IP Address (Destination):** The destination IP address of the host or the network.
- **Subnet Netmask:** Select a destination subnet netmask of the host or the network.
- **IP Address (Gateway):** The IP address of the next router to the destination.

- **Maximum Concurrent Session for User:** Include Maximum Concurrent Session for User, from 10 to Unlimited. The concurrent sessions for each user, it can be restricted by administrator.

Note: *For more information, please refer to* ***Appendix E. Session Limit and Session Log****.*

4.2.4.2 Policy 1 ~ Policy 12

Polices can be defined in the Policy tab. The administrator can select one of the defined policies to apply it to the specific authentication option. All clients belong to this authentication option will be bound by this policy. A policy could be applied at zone level, at group level or at user level. User level policy overrides group level policy. Group level policy overrides zone level policy. Zone level policy overrides the global policy.

When the type of authentication database is "Local", a policy is applied at per user basis. When the type of database is NTDOMAIN or ONDEMAND, a policy is applied to the whole user database. When type of database is RADIUS, a policy is mapped to a user group of a RADIUS class. The Class-Policy Mapping function will be available to let the administrator assign a policy for a RADIUS Class attribute. When the type of database is LDAP, a policy is applied to user group defined an attribute-value pair. The Attribute-Policy Mapping function will be available to let administrator assign a policy for a LDAP Attribute. When the type of database is SIP, the Policy selection function will be available to let the administrator assign a policy for all SIP users.

Policy Configuration - Policy 1	
Select Policy:	Policy 1
Firewall Profile	Setting
Specific Route Profile	Setting
Schedule Profile	Setting
Maximum Concurrent Sessions	500 (Sessions per User)

- **Select Policy:** Select a *Policy* for further configuration. Below depicts an example of selecting *Policy 1*.
- **Firewall Profile:** Each Policy has a firewall service list and a set of firewall profile consisting of firewall rules.
- **Select Policy:** Select **Policy1~Policy12** to set the **Firewall Profile**, **Specific Route Profile, Schedule Profile** and **Maximum Concurrent Session**.
- **Firewall Profile:** Each Policy has a firewall service list and a set of firewall profile consisting of firewall rules.
- **Specific Route Profile:** The default gateway of WAN1, WAN2, or a desired IP address can be defined in a policy. When Specific Default Route is enabled, all clients applied this policy will access the Internet through this default gateway.
- **Schedule Profile:** The Schedule table in a 7X24 format is used to control the clients' login time. When Schedule is enabled, clients applied policies are only allowed to login the system at the time which is checked in the applied policy.
- **Maximum Concurrent Sessions:** Set the maximum concurrent sessions for each client.

- **Firewall Profile:** Click ***Setting*** for **Firewall Profile**. The Firewall Configuration will appear. Click **Predefined and Custom Service Protocols** to edit the protocol list. Click **Firewall Rules** to edit the rules.

Policy 1 - Firewall Configuration
Predefined and Custom Service Protocols
Firewall Rules

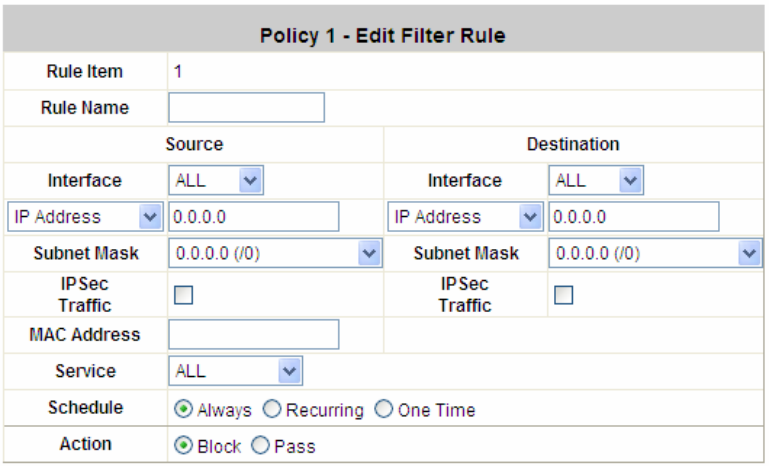
o **Predefined and Custom Service Protocols:** This link leads to a Service Protocols List where the administrator can defined a list of service by protocols (TCP/UDP/ICMP/IP). There are predefined service protocols available for firewall rules editing. The administrator is able to add new customized service protocols by clicking ***Add***, and delete the added protocols by clicking ***Delete***.

Policy 1 - Service Protocols List			
No.	Name	Description	Select All
1	ALL	ALL	☐
2	ALL TCP	TCP; Source Port: 0~65535, Destination Port: 0~65535	☐
3	ALL UDP	UDP; Source Port: 0~65535, Destination Port: 0~65535	☐
4	ALL ICMP	ICMP; Type: Any, Code: Any	☐
5	FTP	TCP/UDP; Destination Port: 20;21	☐
6	HTTP	TCP/UDP; Destination Port: 80	☐
7	HTTPS	TCP/UDP; Destination Port: 443	☐
8	POP3	TCP; Destination Port: 110	☐
9	SMTP	TCP; Destination Port: 25	☐
10	DHCP	UDP; Destination Port: 67;68	☐

o **Firewall Rules:** Click on the hyperlink in the **No.** column to edit individual rules and then click ***Apply*** to save the settings. The rule status will show on the list. Check the *Active* check box and click ***Apply*** to enable that rule. This link leads to the **Firewall Rules** page. Rule No.1 has the highest priority; Rule No.2 has the second priority and so on. Each firewall rule is defined by **Source**, **Destination** and **Pass/Block** action. Optionally, a Firewall Rule Schedule can be set to specify when the firewall rule is enforced. It can be set to *Always*, *Recurring* or *One Time*.

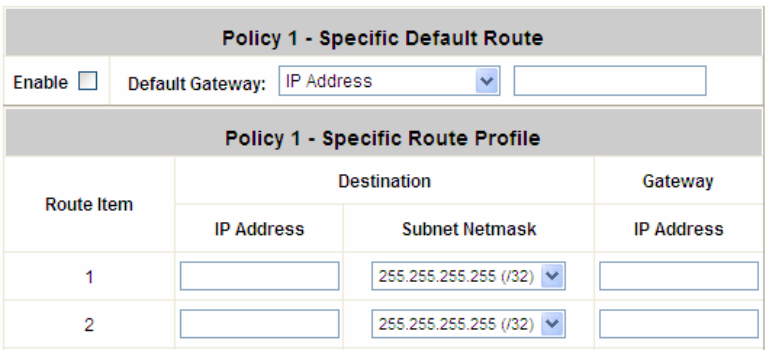
Policy 1 - Firewall Rules							
No.	Active	Action	Name	Source	IPSec Encrypted	Service	Schedule
				Destination	IPSec Encrypted		
1	☐	Block		ANY		ALL	Always
				ANY			
2	☐	Block		ANY		ALL	Always
				ANY			

Below depicts an example of selecting Filter Rule Number 1:



- **Rule Item:** This rule number of the selected rule. Rule No. 1 has the highest priority; Rule No. 2 has the second priority, and so on.
- **Rule Name:** The rule name can be changed here.
- **Source / Destination – Interface/Zone**: There are choices of *ALL*, *WAN1*, *WAN2*, *Default* and the *Service Zones* to be applied to the traffic interface.
- **Source / Destination – IP Address/Domain Name:** Enter the source and destination IP addresses.
- **Source / Destination – Subnet Mask:** Enter the source and destination subnet masks.
- **Source / MAC Address:** The MAC Address of the source IP address. This is for specific MAC address filter.
- **Source / Destination – IPSec Traffic:** Check the box to filter the encrypted traffic only.
- **Service Protocol:** Select a defined protocol from the drop-down list box.
- **Schedule:** Defines the time when this firewall rule will be activated. When a schedule is selected, the clients assigned to this Policy are applied with the firewall rule only within the time selected. There are three options, *Always*, *Recurring* and *One Time*.
- **Action for Matched Packets:** There are two options, *Block* and *Pass*. Block is to prevent packets from passing, while Pass is to permit packets passing.

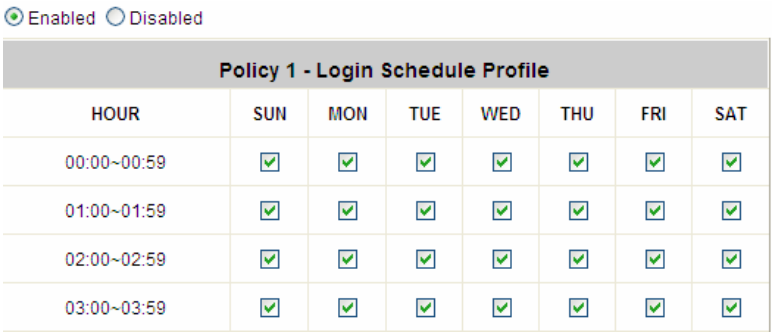
➢ **Specific Route Profile:** The default gateway of WAN1, WAN2, or a desired IP address can be defined in a Policy. When Specific Default Route is enabled, all clients applied with this Policy will access the Internet through this default gateway.



Click ***Setting*** of *Specific Route Profile* to enter the **Specific Route** page for further configuration.

- **Enable:** Check ***Enable*** box to activate this function or uncheck to inactivate it.
- **Destination / IP Address:** The destination network address or IP address of the destination host. Please note that, if applicable, the system will calculate and display the appropriate value based on the combination of Network/IP Address and Subnet Mask that are just entered and applied.
- **Destination / Subnet Netmask:** The subnet mask of the destination network. Select *255.255.255.255(/32)* if the destination is a single host.
- **Gateway / IP Address:** The IP address of the gateway or next router to the destination.

➢ **Schedule Profile:** Click ***Setting*** of *Schedule Profile* to enter the configuration page. Select ***Enable*** to show the **Permitted Login Hours** list. This function is used to limit the time when clients can log in. Check the desired time slots and click ***Apply*** to save the settings. These settings will become effective immediately after clicking ***Apply***.



➢ **Maximum Concurrent Session for User:** Include Maximum Concurrent Session for User, from 10 to Unlimited. The concurrent sessions for each user, it can be restricted by administrator.

Note: *For more information, please refer to* ***Appendix E. Session Limit and Session Log****.*

4.2.5 Additional Configuration

Additional Configuration	
User Control	Idle Timer: 10 *(Range: 1-1440) Multiple Login ☐ (On-demand and RADIUS authentication do NOT support multiple login.)
Roaming Out Timer	Session Timeout: 120 *(Range: 5-1440) Idle Timeout: 10 *(Range: 1-120) Interim Update: 5 *(Range: 1-120)
Upload File	Certificate
Credit Reminder	Volume ○ Enable ◉ Disable Time ○ Enable ◉ Disable
Enhance User Authentication	Permit MAC Address List (Control list to manage which client devices are allowed to access the login page)

- **User Control:** Functions under this section apply to all general users.

  Idle Timer: If a user has idled with no network activities, the system will automatically kick out the user. The logout timer can be set between 1~1440 minutes, and the default logout time is 10 minutes.

  Multiple Login: When enabled, a user can log in from different computers with the same account. (This function doesn't support On-demand users and RADIUS authentication.)

- **Roaming Out Timer:**

  Session Timeout: The time that the user can access the network while roaming. When the time is up, the user will be kicked out automatically.

  Idle Timeout: If a user has idled with no network activities, the system will automatically kick out the user.

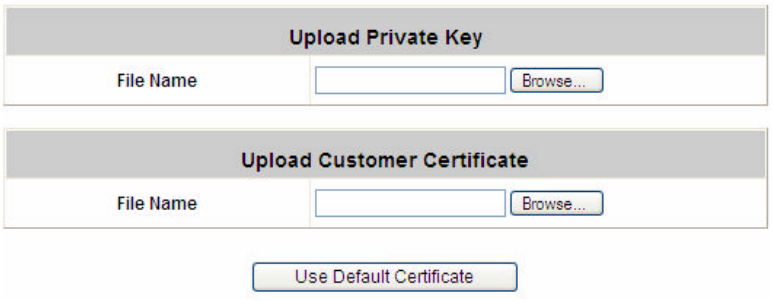
  Interim Update: The system will update the users' current status and usage according to this time period.

- **Upload File**

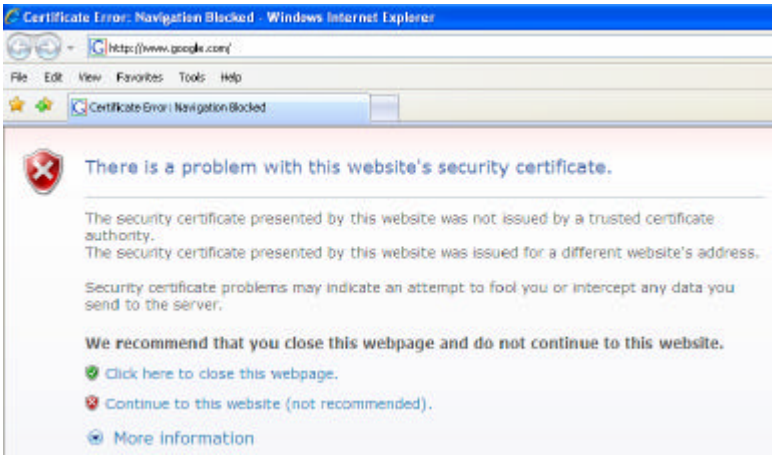
  SSL Certificate

  A data record used for authenticating network entities such as a server or a client. A certificate contains X.509 information pieces about its owner (called the subject) and the signing Certificate Authority (called the issuer), plus the owner's public key and the signature made by the CA. Network entities verify these signatures using CA certificates. You can apply for a SSL certificate at CAs such as VeriSign.

  If you already have an SSL Certificate, please Click Browse to select the file and upload it. Click ***Apply*** to complete the upload process.

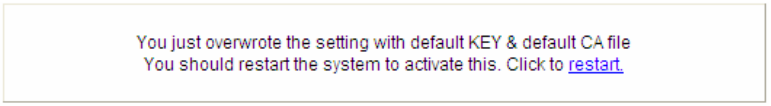


Without a valid certificate, users may encounter the following problem in IE7 when they try to open the login page.

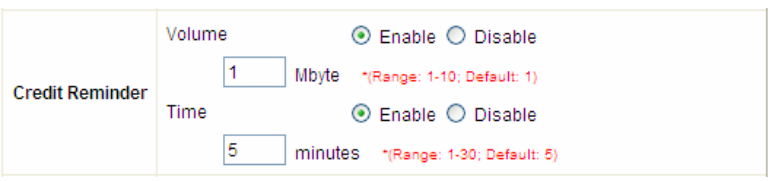

Certificate Error: Navigation Blocked - Windows Internet Explorer
File Edit View Favorites Tools Help
Certificate Error: Navigation Blocked
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

Click "Continue to this website" to access the user login page.

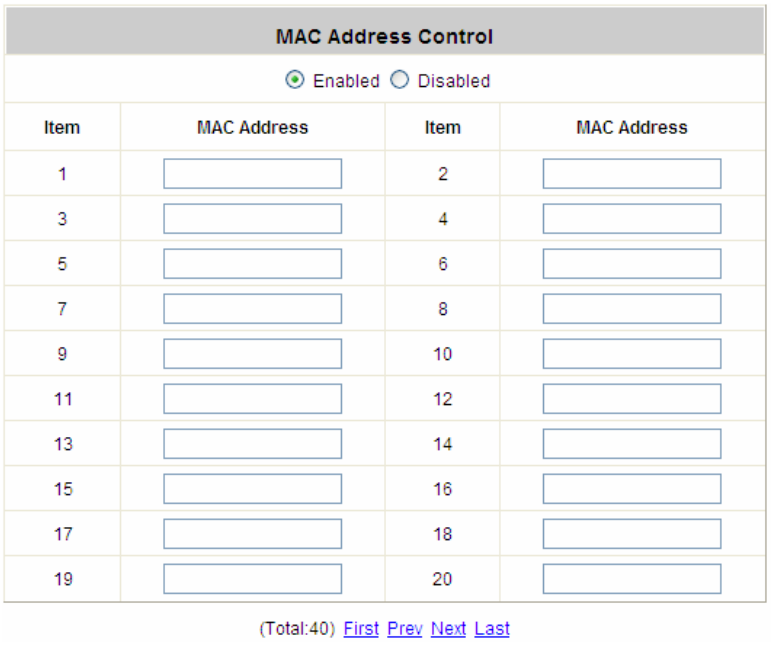
To Use Default Certificate: Click ***Use Default Certificate*** to use the default certificate and key. Click **restart** to validate the changes.


You just overwrote the setting with default KEY & default CA file
You should restart the system to activate this. Click to restart.

- **Credit Reminder:** The administrator can enable this function to remind the on-demand users before their credit run out. There are two kinds of reminder, **Volume** and **Time**. The default reminding trigger level for **Volume** is 1Mbyte and the level for **Time** is 5 minutes.



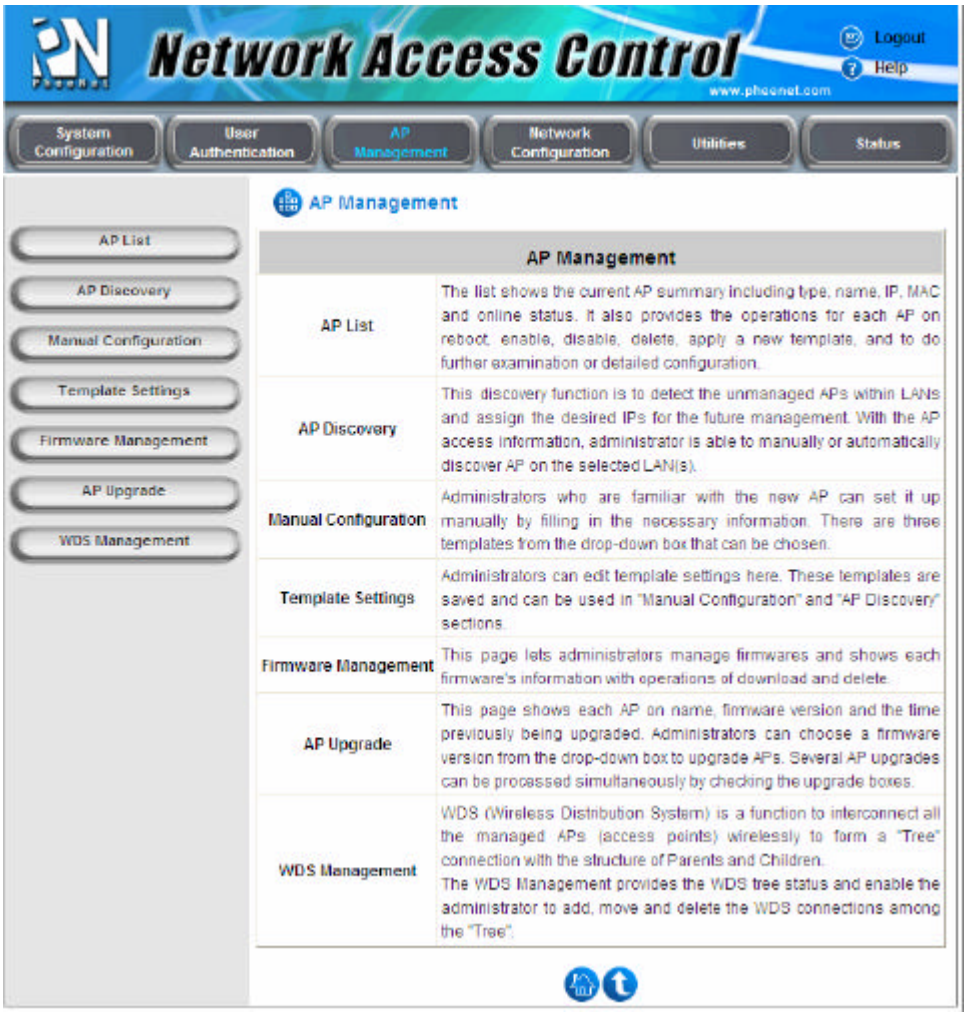
- **Enhance User Authentication:** With this function, only the users with their MAC addresses in this list can log into WMS-208. There are 40 users maximum allowed in this MAC address list. User authentication is still required for these users. Please enter the **Permit MAC Address List** to fill in these MAC addresses, select **Enable**, and then click ***Apply***.



Caution: *The format of the MAC address is: xx:xx:xx:xx:xx:xx or xx-xx-xx-xx-xx-xx.*

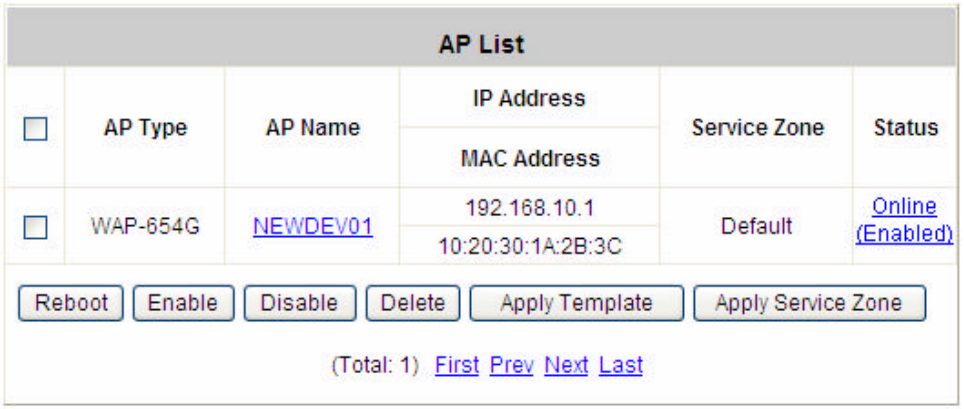
4.3 AP Management

WMS-208 supports to manage up to 12 access points (AP), and they can be configured in this section. This section includes the following functions: **AP List**, **AP Discovery**, **Manual Configuration**, **Template Settings**, **Firmware Management**, **AP Upgrade** and **WSD Management**.


Network Access Control
www.pheenet.com
Logout
Help
System Configuration
User Authentication
AP Management
Network Configuration
Utilities
Status
AP List
AP Discovery
Manual Configuration
Template Settings
Firmware Management
AP Upgrade
WDS Management
AP Management
AP Management
AP List
The list shows the current AP summary including type, name, IP, MAC and online status. It also provides the operations for each AP on reboot, enable, disable, delete, apply a new template, and to do further examination or detailed configuration.
AP Discovery
This discovery function is to detect the unmanaged APs within LANs and assign the desired IPs for the future management. With the AP access information, administrator is able to manually or automatically discover AP on the selected LAN(s).
Manual Configuration
Administrators who are familiar with the new AP can set it up manually by filling in the necessary information. There are three templates from the drop-down box that can be chosen.
Template Settings
Administrators can edit template settings here. These templates are saved and can be used in "Manual Configuration" and "AP Discovery" sections.
Firmware Management
This page lets administrators manage firmwares and shows each firmware's information with operations of download and delete.
AP Upgrade
This page shows each AP on name, firmware version and the time previously being upgraded. Administrators can choose a firmware version from the drop-down box to upgrade APs. Several AP upgrades can be processed simultaneously by checking the upgrade boxes.
WDS Management
WDS (Wireless Distribution System) is a function to interconnect all the managed APs (access points) wirelessly to form a "Tree" connection with the structure of Parents and Children.
The WDS Management provides the WDS tree status and enable the administrator to add, move and delete the WDS connections among the "Tree".

4.3.1 AP List

All of the APs under the management of WMS-208 will be shown in the list. The AP can be edited by clicking the hyperlink of ***AP Name*** and the AP status can be got by clicking the hyperlink of ***Status***.



After adding an AP:

Check any AP and click the button below to ***Reboot***, ***Enable***, ***Disable***, ***Delete***, ***Apply Template*** and ***Apply Service Zone*** to the checked AP.

- **AP Name**

  The AP name will be shown as hyperlink. Click the hyperlink of each managed AP can have for configurations about the specific AP. Click the hyperlink of the **AP Name** to have more configurations. There are four kinds of settings available: **General**, **LAN**, **Wireless LAN** and **Access Control**. Click the hyperlink of each individual setting to have further configurations.

- **Service Zone**

  After the AP is added into AP List, the managed AP can be assigned to one or multiple service zone.

- **Status:**

  Each AP's status will be shown in this column. Click the hyperlink of the shown status of each managed AP to see detailed status information about the specific AP, such as System Status, Service Zone Status, Wireless Status, Access Control Status and Associated Client Status. The status includes:

  (1) **Online:** The hyperlink of Online (Enabled) indicates that the AP is currently online and in service; Online (Disabled) indicates that the AP is currently online but not ready in service.

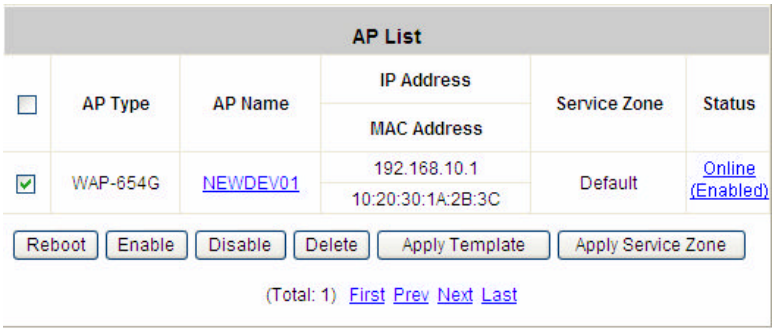
  (2) **Offline:** The AP is currently offline; for example: it is displayed as Offline when the power of the AP is off or the network connection between the AP and the system is down.

  (3) **Configuring:** It is displayed as Configuring when the newly discovered AP is being added to the list (and being configured) or new setting is being applied to the AP.

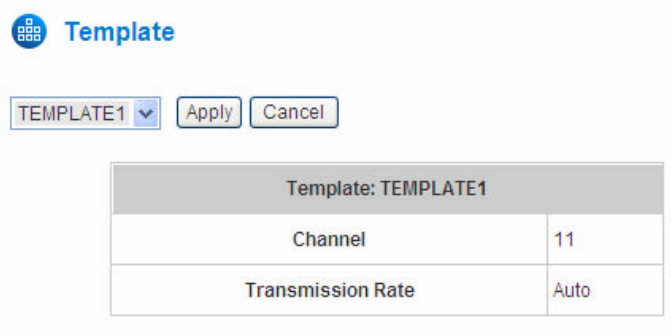
  (4) **Upgrading:** The AP is undergoing firmware upgrade.

  (5) **Lost/Unknown:** After the system's rebooting and before it tries to probe the AP and determine the exact status, the status will be displayed as Lost or Unknown temporarily.

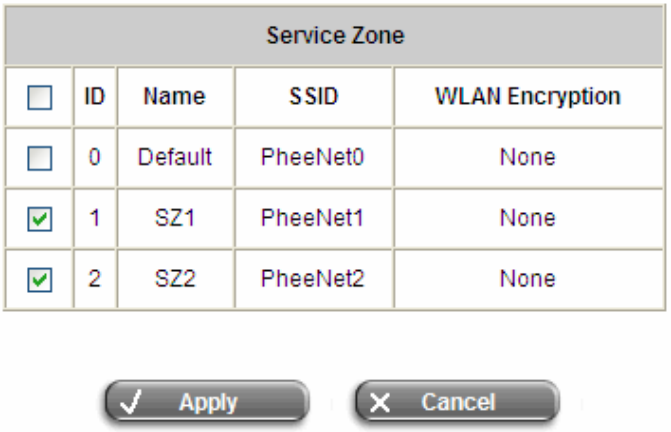
Check any AP and then click the button below to ***Reboot***, ***Enable***, ***Disable*** and ***Delete*** the checked AP if desired.



Click ***Apply Template*** to select one template to apply to the AP.



Click ***Apply Service Zone*** to setup one Service Zone to the AP.



- **AP Name**

  Click ***AP Name*** and enter the interface about related settings. There **are** four kinds of settings, **General Settings**, **LAN Interface Setting**, **Wireless Interface Setting** and **Access Control Setting**. Click the hyperlink to go on the configuration.

General Settings		
General	Name	NEWDEV02
	Firmware	Unknown

LAN Interface Settings		
LAN	IP	192.168.10.2
	Gateway	192.168.10.254

Wireless Interface Settings		
Wireless LAN	Channel	Auto
	Data Rate	Auto

Access Control Settings		
Access Control	Status	Disabled
	Number of MAC Addresses	0

  - **General Setting:** Click ***Setting*** to enter the **General Setting** interface. Firmware information can be observed here.

General Settings	
Name	Eric_1 *
Admin Password	*****
NTP	Time Zone (GMT+08:00)Taipei,Taiwan NTP Server 1: tick.stdtime.gov.tw * NTP Server 2: tock.stdtime.gov.tw
SNMP	Disabled
SYSLOG	Disabled
Firmware	1.00.00

- **LAN Setting:** Click ***LAN*** to enter the **LAN Setting** interface. Input the data of LAN including **IP address**, **Subnet Mask** and **Default Gateway** of AP.

LAN Settings	
IP Address	192.168.1.1 *
Subnet Mask	255.255.255.0 *
Default Gateway	192.168.1.254 *
Primary DNS	192.168.1.254 *
Secondary DNS	

- **Wireless LAN:** Click ***Wireless LAN*** to enter the **Wireless** interface. The data of Properties and Security need to be filled.

Wireless	
SSID Broadcast	Enabled
Channel	Auto
Wireless b/g mode	802.11b
Data Rate	Auto
Fragment Length	2346 (Default: 2346; Range: from 256 to 2346)
RTS Threshold	2346 (Default: 2346; Range: from 1 to 2346)
Beacon Interval (ms)	100 (Default:100 ; Range: from 25 to 500)
Preamble	Long Only
Transmit Power	Auto
Wireless QoS WMM	Enabled
Wireless Client Isolation	Disabled
IAPP	Enabled

Properties

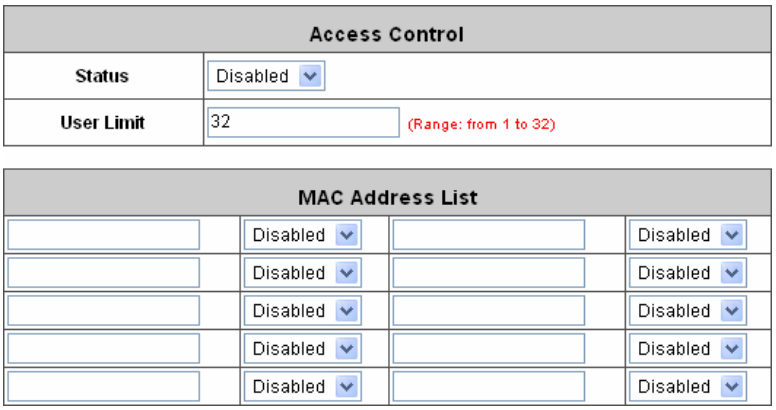
- **SSID Broadcast:** Select this option to enable the SSID to broadcast in the network. When configuring the network, it's suggested to enable this function but also make sure to disable it when finished. With this enabled, someone could easily obtain the SSID information with the site survey software and get unauthorized access to an individual's network. With this disabled to increase network security and prevent the SSID from being seen on networked.
- **Channel:** Select the appropriate channel from the list to correspond with the network settings; for example, 1 to 11 channels are suitable for the North America area.
- **Wireless b/g Mode:** There are 3 modes to select from, **802.11b** (2.4G, 1~11Mbps), **802.11g** (2.4G, 54Mbps) and **802.11b+802.11g** (b and g).
- **Data Rate:** The default is **Auto**. Available range is from 1 to 54Mbps. The rate of data transmission should be set depending on the speed of the wireless network. Select from a range of transmission speed is desired or keep the default setting, **Auto**, to make the Access Point automatically use the fastest rate possible.
- **Fragment Length:** Breaking a packet into smaller units when transmitting over a network medium that

cannot support the original size of the packet.

- **RTS Threshold:** Enter the desired RTS Threshold value, the range is from 0 to 2347, and the default is 2347.
- **Beacon Interval (ms):** Enter a value between 20 and 1000 msec. The default value is 100 milliseconds. The entered time means how often the beacon signal transmits between the access point and the wireless network.
- **Preamble:** Select from either Short Preamble or Long Preamble; the short preamble provides 56 bits Synchronization field to improve WLAN transmission efficiency.
- **Transmit Power:** Choose the suitable value from the drop-down box.
- **Wireless QoS WMM:** Enable or disable QoS and WMM. WMM maintains the priority of audio, video and voice applications in a Wi-Fi network so that other applications and traffic are less likely to slow them.
- **Wireless Client Isolation:** Enable or disable Client Isolation. Client Isolation prevents wireless client to client traffic.
- **IAPP:** Inter Access-Point Protocol is designed for the enforcement of unique association throughout a ESS (Extended Service Set) and for secure exchange of station's security context between current access point (AP) and new AP during handoff period.

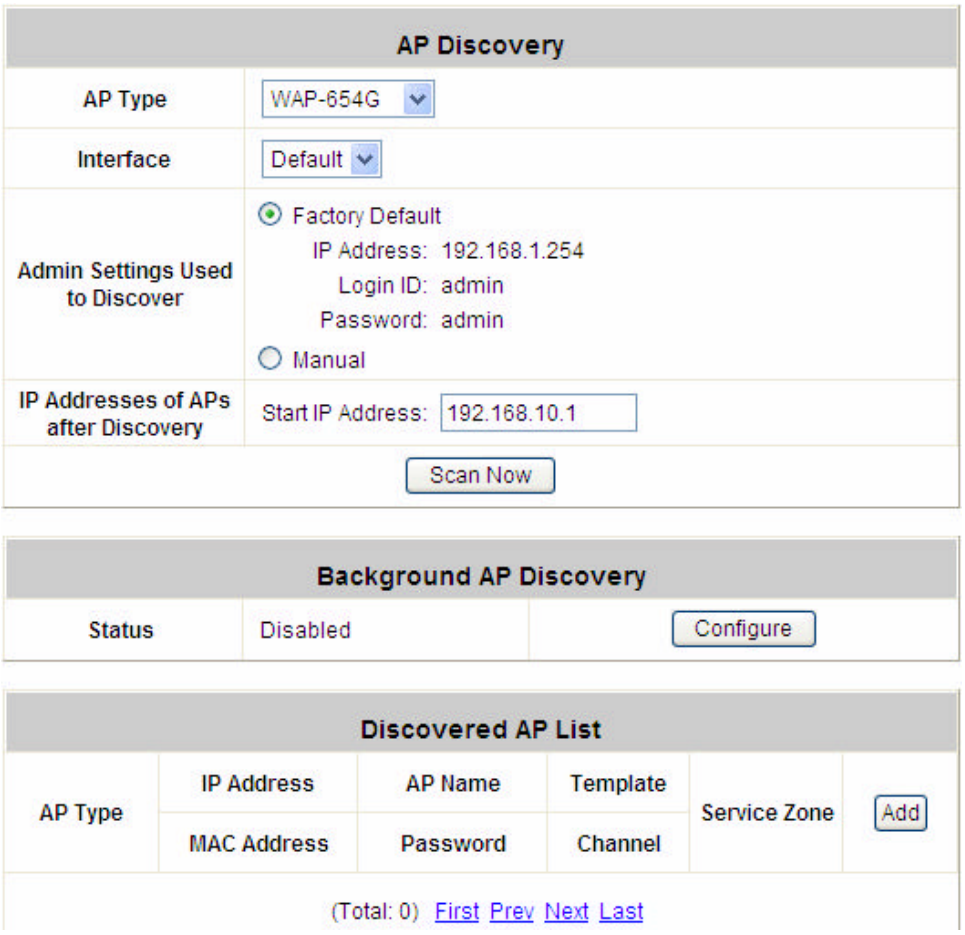
➢ **Access Control:** In this function, when the status is **"Allowed"**, only these clients whose MAC addresses are listed in this list can be allowed to connect to the AP; on the other hand, when the status is "Denied", the clients whose MAC addresses are listed in the list will be denied to connect to the AP. When **"Disabled"** is selected, all clients can connect to the AP. The default is **Disabled**.

- **User Limit:** Limit the number of users connected to that AP.



4.3.2 AP Discovery

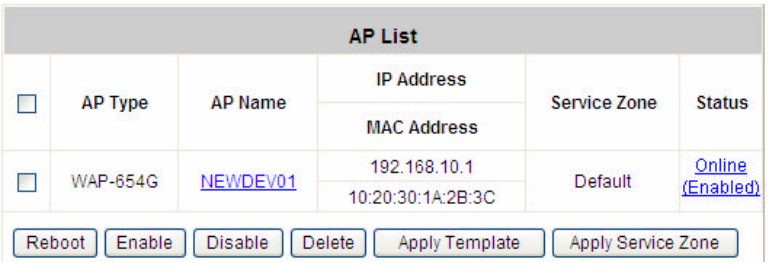
Use this function to detect and manage all of the APs in the network segments. Note that WMS-208 can only manage APs that are connected to its LAN ports. Therefore, the AP discovery function is for adding locally connected APs to its management list. The administrator must know the local IP addresses of the APs he/she wishes to discover.



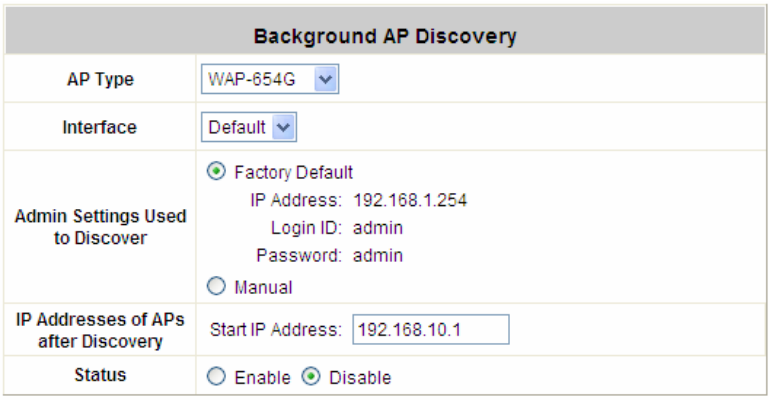
- To discover AP manually, please fill in the required data.
  - **AP Type:** Choose the type of AP you wish to discover.
  - **Interface:** Set to default.
  - **Admin Settings Used to Discover:** Choose from Factory Default or Manual.
  - **IP Addresses of APs after Discovery:** Start assigning from this IP address to discovered APs.

  Then click the ***Scan Now*** button and the APs match the given settings will show in the list below. If one of the IP addresses intended is used, a warning message will show up. In this case, please change the IP range and then click ***Scan Now*** again. Input the desired name and password for the AP. Select one template check it and then click ***Add*** to add it under the managed list. (About the template, please see 4.3.4 Template Settings).
  When the matched AP is discovered, it will show up in the list below and be given a new IP address set here (ex: 192.168.2.2). Check the **Add** box to add the AP and it will be listed to the AP list. When an AP is added, its MAC address will be automatically recorded into MAC Privilege List (please see 4.4.2 Privilege List) so its management page can be accessed.

Click Configuring to go on the related configuration. For the details, please refer to **4.3.1 AP List**.



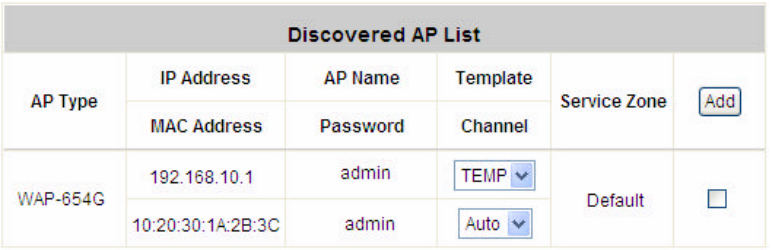
- **Background AP Discovery:** Click ***Configure*** to enter Background AP Discovery interface to go on related configuration.



The **Interface** and **AP Access** configuration is the same as the settings mentioned above. When **Background AP Discovery** function is enabled, the system will scan once every 10 minutes or according to the time set by the administrator. If any AP is discovered and "Auto-Add AP" is enabled, it will be assigned an available IP from the starting IP address and apply the selected template. You can also set the channel the AP would use.

Caution: *The scanning process may take a long time if the IP range assigned to scan is too wide.*

- **Discovered AP List:** The discovered new APs will be listed here. When the system's Service Zone is set to Tag-based mode, service zones also can be assigned here. After clicking ***Add***, the current management page is directed to AP List, where the newly added APs will show up with a status of "configuring". It may take a couple of minutes to see the status of the newly added AP to change from "configuring" to "online" or "offline".



Discovered AP List					
AP Type	IP Address	AP Name	Template	Service Zone	Add
	MAC Address	Password	Channel		
WAP-654G	192.168.10.1	admin	TEMP	Default	☐
	10:20:30:1A:2B:3C	admin	Auto		

  - **AP Type**: This is the supported type of APs for centralized management.
  - **IP Address:** IP address of the specified AP.
  - **MAC Address:** MAC address of the specific AP.
  - **AP Name:** Mnemonic name of the specific AP.
  - **Admin Password:** Password required for this AP.
  - **Template:** The template which will be applied to the added AP.
  - **Channel:** The selected channel will be applied to the added AP.
  - **Service Zone:** Select the name of Service Zone such as Service Zone 1, Guest or Employee.
  - **Add:** The administrator can click ***Add*** button to register the APs to the ***List*** for management.

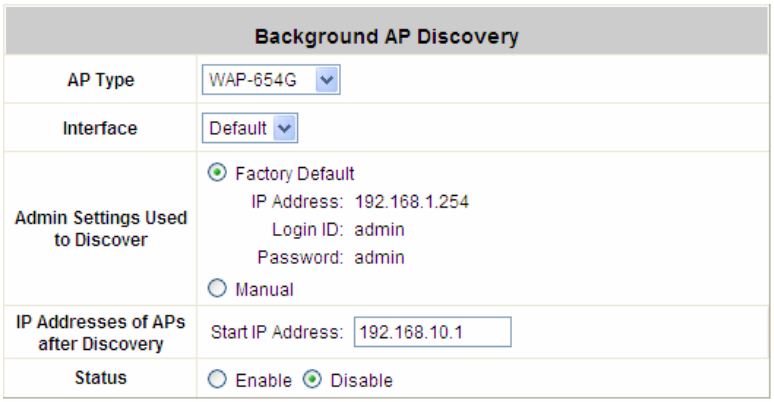
- **Tag-Based and Port-based Configuration in AP Discovery screen:**

Note: *After when configures service zones setting and port/tag-based Mapping in* ***4.1.6 LAN Port Mapping*** *and* ***4.1.7 Service Zones****, the administrator continues to configure* ***AP Discovery*** *settings in* ***AP Management****, while AP Discovery settings differ for port-based and tag-based mode. For complete settings for both port and tag-based mode, please refer to* ***Appendix C. Service Zone Deployment Example****.*

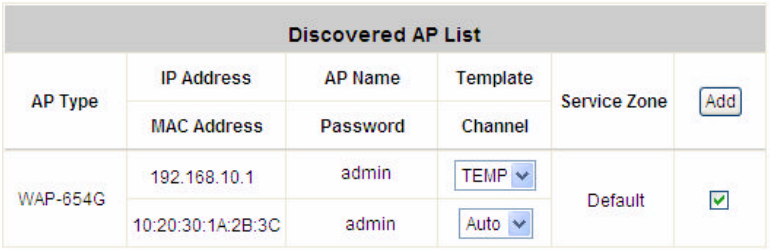
In port-based mode, a new AP must be placed under the Default port only for discovery and then add the AP into other zone. In tag-based mode, a new AP must be placed under any selected port for discover and then select the desired zones before adding the AP into the list.

  - **Step 1:** Configure the mode of **LAN Port Mapping** and **Service Zones** (such as Guest and Employee) in **System Configuration**. (See Appendix C. for further information)
  - **Step 2:** Select **AP Discovery** in **AP Management**
    - **Port-Based mode:**

      In Port-based mode, set the Interface in Default port. Select **Default** in Interface. Select Factory Default in the section of Admin Setting (Recommended). If using the certain range of IP address, type the address in Manual selection. Then, start scanning the new APs in the specific range of IP addresses by clicking ***Scan Now*** button.

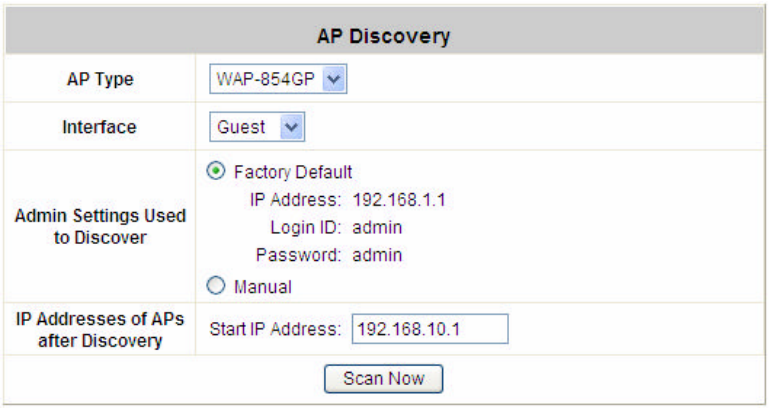


After scanning, new APs will be listed in the **Discovered AP List**. Click the desired names of Service Zone for Tag-based mode. Add the selected AP to the list by checking the AP and clicking ***Add*** button.

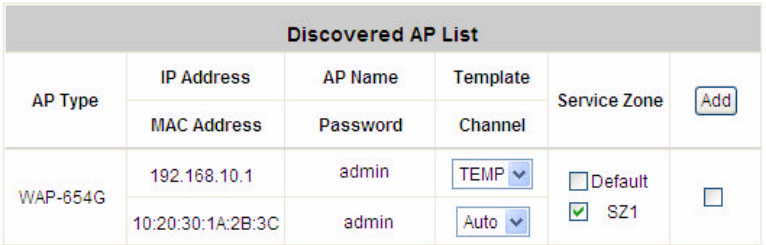


o **Tag-Based mode:**

In Tag-based mode, the name of service zone has been selected in the Interface, such as Guest or SZ1. Select Factory Default in the section of Admin Setting (Recommended). Then, start scanning the new APs in the IP address by clicking ***Scan Now*** button.

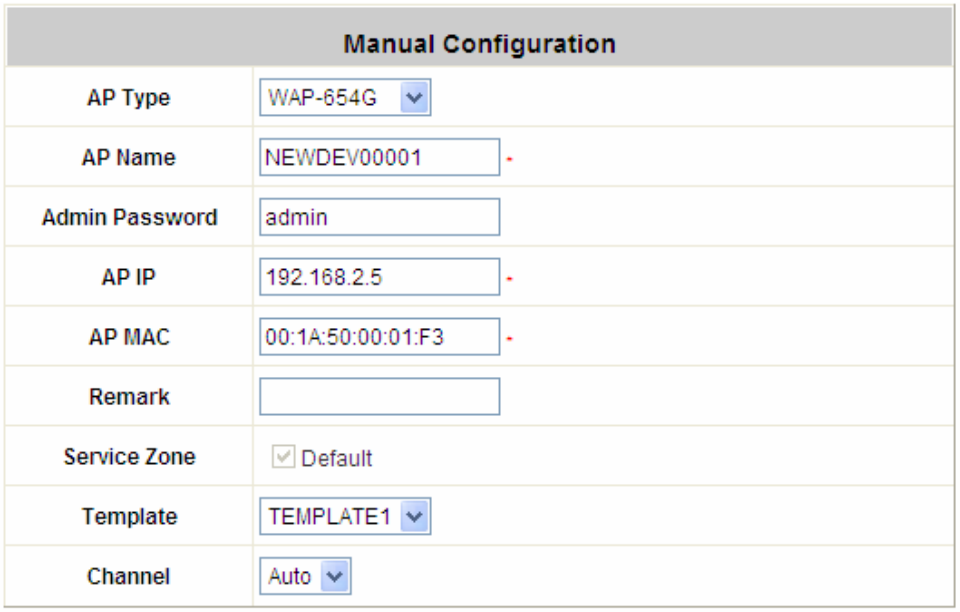


After scanning, new APs will be listed in the **Discovered AP List**. Click the desired names of Service Zone for tag-based mode. Add the selected AP to the list by checking the AP and clicking ***Add*** button.



4.3.3 Manual Configuration

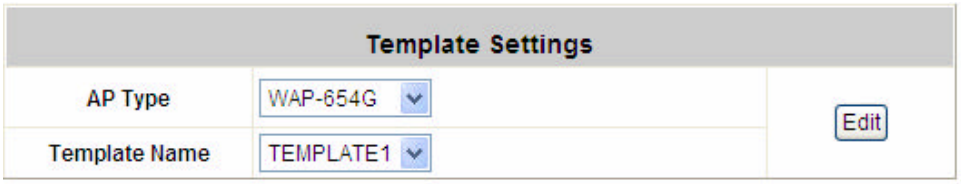
The AP also can be added manually even though when it is offline. Input the related data of the AP and select a Template. After clicking ***Add***, the AP will be added to the managed list.



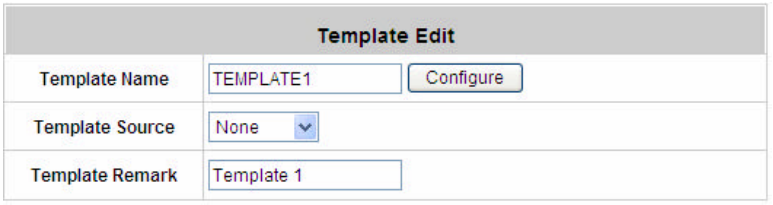
- **AP Type**: This is the supported type of APs for centralized management.
- **AP Name:** Mnemonic name of the specific AP.
- **Admin Password:** Password required for this AP.
- **IP Address:** IP address of the specified AP.
- **MAC Address:** MAC address of the specific AP.
- **Remark:** Some extra information to be filled in for this AP if desired.
- **Service Zone:** The item is only shown when Tag-Based mode is selected in *System Configuration* >> *LAN Port Mapping*. Select the name of Service Zone such as Service Zone 1, Guest or Employee.
- **Template:** The template which will be applied to the added AP.
- **Channel:** The selected channel will be applied to the added AP.

4.3.4 Template Settings

Template is a model that can be copied to every AP and not necessary to configure the AP individually. There are three templates provided. Click ***Edit*** to go on configuration.



Before configure the template, copy the configuration mode of an AP to the template by selecting a **Source AP**, and without configuring the template from the beginning, administrators can also revise some settings for demand. If copy is not desired, please select **NONE**. Input the **Template Name** and **Template Remark** and click the button of ***Configure*** to go on configuration.



- **Template Edit**: Here is the section that administrators can configure template name, template source, and template remark.
- **Template Name**: The name shown for this particular template will change according to what given by administrators.
- **Template Source:** Select an existing AP and click Apply to save its settings as the template settings.

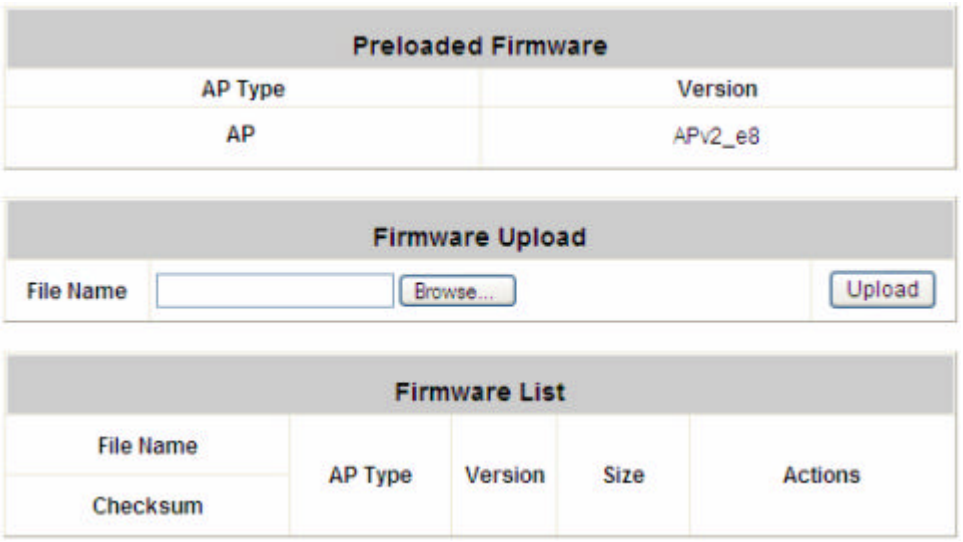
After entering the interface, revise the configuration for demand and change administrator's password if desired. About other function settings, please refer to **4.3.1 AP List**.

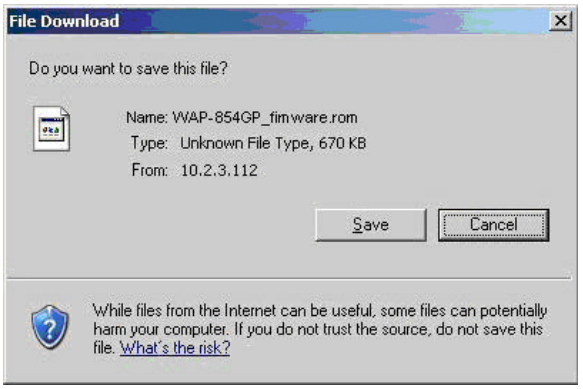
- **Template Editing**

  The administrator can set the template configuration manually. Click ***Configure*** button to have detailed configurations.

4.3.5 Firmware Management

Preloaded Firmware displays the current version of the AP's firmware. New firmware can be uploaded here to update the current firmware. To upload, click Browse to select the file and then click Upload.




File Download
Do you want to save this file?
Name: WAP-854GP_firmware.rom
Type: Unknown File Type, 670 KB
From: 10.2.3.112
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not save this file. What's the risk?

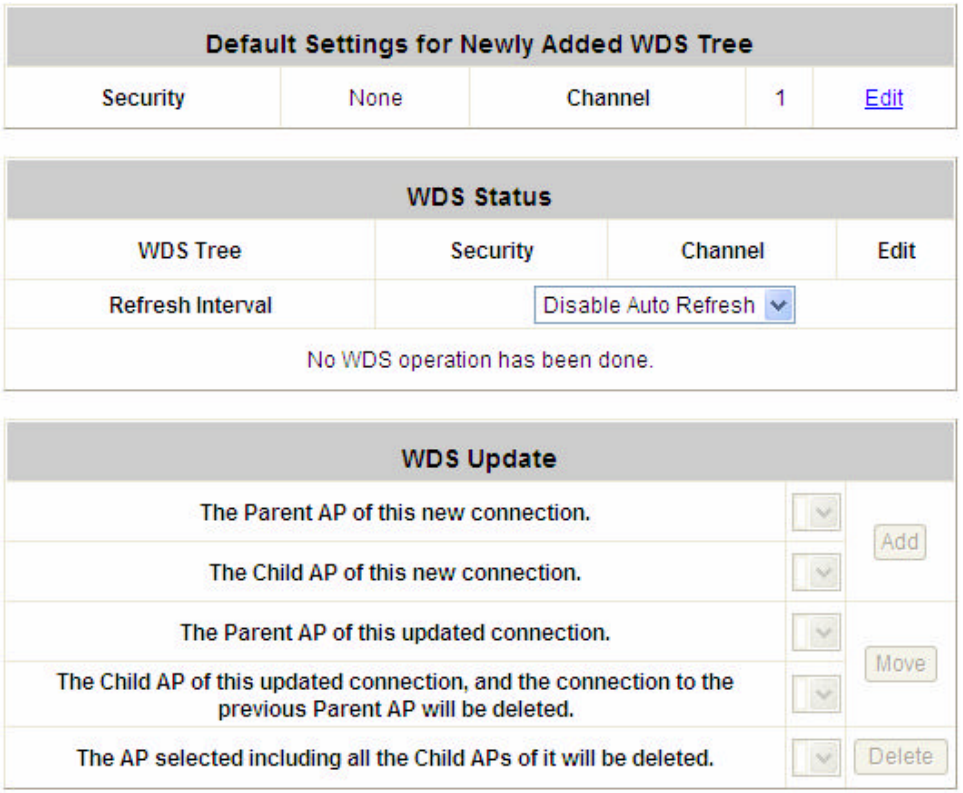
4.3.6 AP Upgrade

Check the APs which need to be upgraded and select the upgrade version of firmware, and click ***Apply*** to upgrade firmware.

AP List					
Name	Type	Version	Upgraded Time	New Version	Upgrade

4.3.7 WDS Management

WDS Management (Wireless Distribution System) is a function used to connect **AP**s (Access Points) wirelessly. The WDS management function of the system can help administrators to setup a WDS network topology.



- **WDS Status:** Status shows the added APs in the WDS Tree with the Security and Channel settings. The WDS could be set up more than one tree. Clicking the ***Edit*** is to change the **WDS connection settings** for the associated WDS Tree.
- **WDS Update:** Update the WDS connection with the following operations.
  - ***Add*****:** Add a new WDS connection with a Child AP not in the WDS and a Parent AP from the AP List. A new WDS Tree will be added if the selected Parent AP is not in any of the current WDS Trees. Clicking ***Edit*** is to change the **WDS connection settings** for the new added WDS Tree.
  - ***Move*****:** Update a WDS connection with a Child AP from WDS and a Parent AP which could be anyone from WDS, and the previous WDS connection of the Child AP to the previous Parent AP will be deleted.
  - ***Delete*****:** All the WDS connections of the selected AP will be deleted including the WDS connections to its Child APs, and the Child APs without wired connection will become unreachable.

4.4 Network Configuration

This section includes the following functions: **Network Address Translation**, **Privilege List**, **Monitor IP List**, **Walled Garden List**, **Proxy Server Properties**, **Dynamic DNS**, **IP Mobility** and **VPN Configuration**.

Network Access Control
Logout
Help
System Configuration
User Authentication
AP Management
Network Configuration
Utilities
Status
Network Address Translation
Privilege List
Monitor IP List
Walled Garden List
Proxy Server Properties
Dynamic DNS
IP Mobility
VPN Configuration
Network Configuration
Network Configuration
Network Address Translation
WMS-208 provides 3 types of network address translation: DMZ (Demilitarized Zone), Public Accessible Server and IP/Port Redirect.
Privilege List
System provides Privilege IP Address List and Privilege MAC Address List. System will NOT authenticate those listed devices.
Monitor IP List
System can monitor up to 40 network devices online status with an option to add them as public access servers via HTTP or HTTPS. Even under NAT mode, after added the devices as public access servers, the devices can be accessed by clicking the hypertext.
Walled Garden List
Up to 20 hosts' URL could be defined in Walled Garden List. Clients may access these URL without authentication.
Proxy Server Properties
WMS-208 supports up to 10 external proxy servers. System can redirect traffic to external proxy server into built-in proxy server.
Dynamic DNS
WMS-208 supports dynamic DNS (DDNS) feature.
IP Mobility
System supports IP PNP Configuration.
VPN Configuration
Local VPN: an IPSec tunnel can be established between the system and the client located at the LAN side.
Remote VPN: a PPTP tunnel can be established between the system and the remote user over the Internet.
Site-to-Site VPN: an IPSec tunnel can be constructed to be used to connect to other IPSec capable device over the Internet.

4.4.1 Network Address Translation

There are three parts, **Demilitarized Zone**, **Public Accessible Server** and **Port and IP Redirect**, that can be set.

Network Address Translation
DMZ (Demilitarized Zone)
Public Accessible Server
Port and IP Redirect

- **DMZ**

  The system supports up to 40 sets of Internal IP address (LAN) to External IP address (WAN) mapping in the Static Assignments. The External IP Address of the Automatic WAN IP Assignment is the IP address of External Interface (WAN1) that will change dynamically if WAN1 Interface is Dynamic. When **Automatic WAN IP Assignments** is enabled, the entered Internal IP Address of Automatic WAN IP Assignment will be bound with WAN1 interface. Each **Static Assignment** could be bound with the chosen External Interface, WAN1 or WAN2. There are 40 sets of static **Internal IP Address** and **External IP Address** available. Enter **Internal** and **External** IP Addresses as a set. After the setup, accessing the WAN will be mapped to access the Internal IP Address. These settings will become effective immediately after clicking the ***Apply*** button.

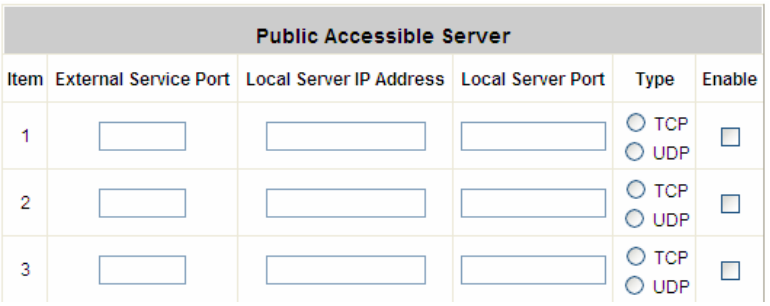
Automatic WAN IP Assignment			
Enable	External IP Address	External Interface	Internal IP Address
☐		WAN1	

Static Assignments			
Item	External IP Address	External Interface	Internal IP Address
1		WAN1	
2		WAN1	
3		WAN1	
4		WAN1	
5		WAN1	
6		WAN1	
7		WAN1	
8		WAN1	
9		WAN1	
10		WAN1	

(Total:40) First Prev Next Last

- **Public Accessible Server**

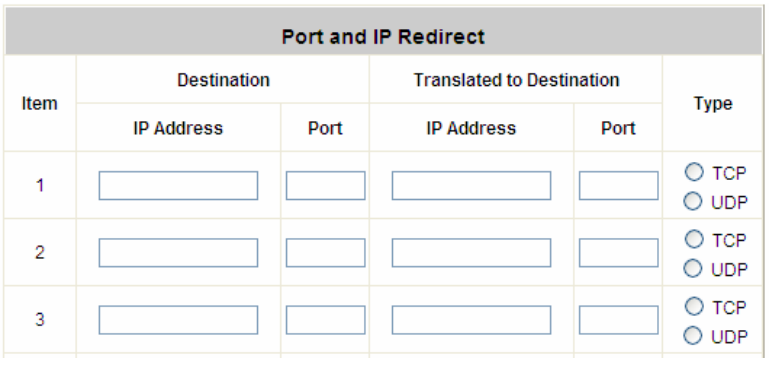
  This function allows the administrator to set 40 virtual servers at most, so that client devices outside the managed network can access these servers within the managed network. Different virtual servers can be configured for different sets of physical services, such as TCP and UDP services in general. Enter the **"External Service Port"**, **"Local Server IP Address"** and **"Local Server Port"**. Select **"TCP"** or **"UDP"** for the service's type. In the **Enable** column, check the desired server to enable. These settings will become effective immediately after clicking the ***Apply*** button.



Public Accessible Server					
Item	External Service Port	Local Server IP Address	Local Server Port	Type	Enable
1				TCP UDP	
2				TCP UDP	
3				TCP UDP	

- **Port and IP Redirect**

  This function allows the administrator to set 40 sets of the IP addresses maximum for redirection purpose. When the user attempts to connect to a destination IP address listed here, the connection packet will be converted and redirected to the corresponding destination. Please enter the **"IP Address"** and **"Port"** of **Destination**, and the **"IP Address"** and **"Port"** of **Translated to Destination**. According to the different services provided, choose the **"TCP"** protocol or the **"UDP"** protocol. These settings will become effective immediately after clicking ***Apply***.



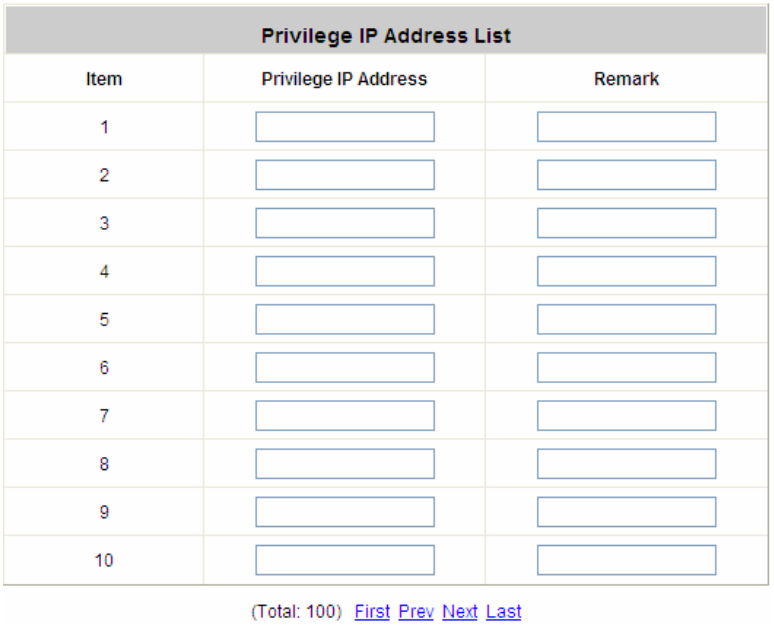
Port and IP Redirect					
Item	Destination		Translated to Destination		Type
	IP Address	Port	IP Address	Port	
1					TCP UDP
2					TCP UDP
3					TCP UDP

4.4.2 Privilege List

There are two parts, **Privilege IP Address List** and **Privilege MAC Address List**, which can be set.

- **Privilege IP Address List**

  If there are some workstations belonging to the managed server that need to access the network without getting authenticated, enter the IP addresses of these workstations in this list. The **"Remark"** blank is not necessary to be filled in but is useful in record-keeping. WMS-208 allows 100 privilege IP addresses at most. These settings will become effective immediately after clicking ***Apply***.



Warning: *Permitting specific IP addresses to have network access rights without going through standard authentication process at the controlled port may cause security problems.*

- **Privilege MAC Address List**

  In addition to the IP address, the MAC address of the workstations that need to access the network without getting authenticated can also be set in this list. WMS-208 allows 100 privilege MAC addresses at most.
  It is possible to manually create the list by entering the MAC address (the format is xx:xx:xx:xx:xx:xx) as well as entering the remark (not required). These settings will become effective immediately after clicking ***Apply***.

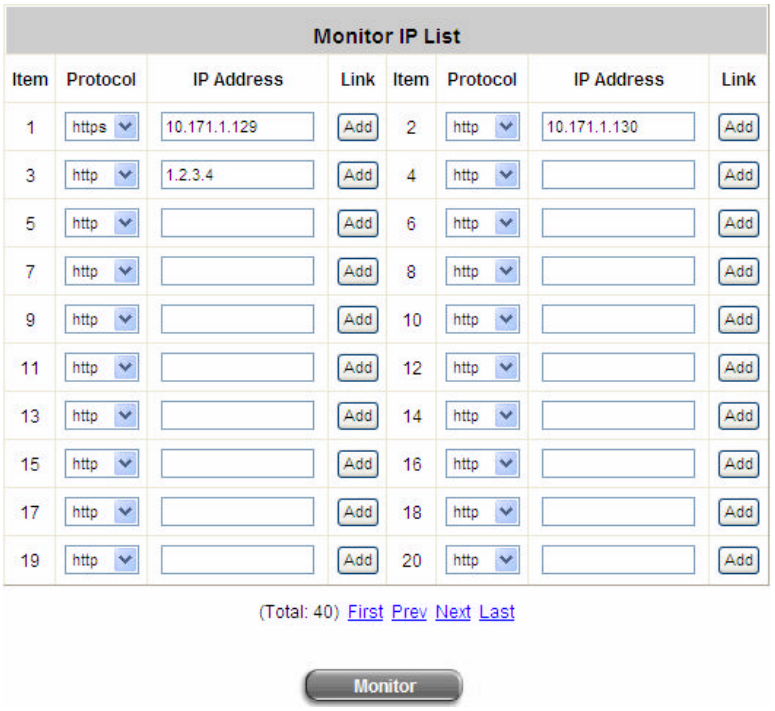
Privilege MAC Address List		
Item	MAC Address	Remark
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

(Total: 100) First Prev Next Last

Warning: *Permitting specific MAC addresses to have network access rights without going through standard authentication process at the controlled port may cause security problems.*

4.4.3 Monitor IP List

WMS-208 will send out a packet periodically to monitor the connection status of the IP addresses on the list. If the monitored IP address does not respond, the system will send an e-mail to notify the administrator that such destination is not reachable. After entering the related information, click ***Apply*** and these settings will become effective immediately. Click ***Monitor*** to check the current status of all the monitored IPs. Green light means online and red light means offline. The system provides 40 monitor IP address fields on the **"Monitor IP List"**.


Monitor IP List
Item Protocol IP Address Link Item Protocol IP Address Link
1 https 10.171.1.129 Add 2 http 10.171.1.130 Add
3 http 1.2.3.4 Add 4 http Add
5 http Add 6 http Add
7 http Add 8 http Add
9 http Add 10 http Add
11 http Add 12 http Add
13 http Add 14 http Add
15 http Add 16 http Add
17 http Add 18 http Add
19 http Add 20 http Add
(Total: 40) First Prev Next Last
Monitor

On each monitored item with a WEB server running, administrators may add a link for the easy access by selecting a protocol, http or https, and click the ***Add*** button. After clicking ***Add*** button, the IP address will become a hyperlink, and administrators can easily access the host by clicking the hyperlink remotely. Click the ***Del*** button to remove the setting.

4.4.4 Walled Garden List

This function provides some free services to the users to access websites listed here before login to the network and without being authenticated. Up to 20 addresses or domain names of the websites can be defined in this list. Users without the network access right can still have a chance to experience the actual network service free of charge. Enter the website **IP Address** or **Domain Name** in the list and these settings will become effective immediately after clicking ***Apply***.

Walled Garden List			
Item	Address	Item	Address
1		2	
3		4	
5		6	
7		8	
9		10	
11		12	
13		14	
15		16	
17		18	
19		20	

Caution: *To use the domain name, the WMS-208 has to connect to DNS server first or this function will not work.*

4.4.5 Proxy Server Properties

WMS-208 supports Internal Proxy Server and External Proxy Server functions.

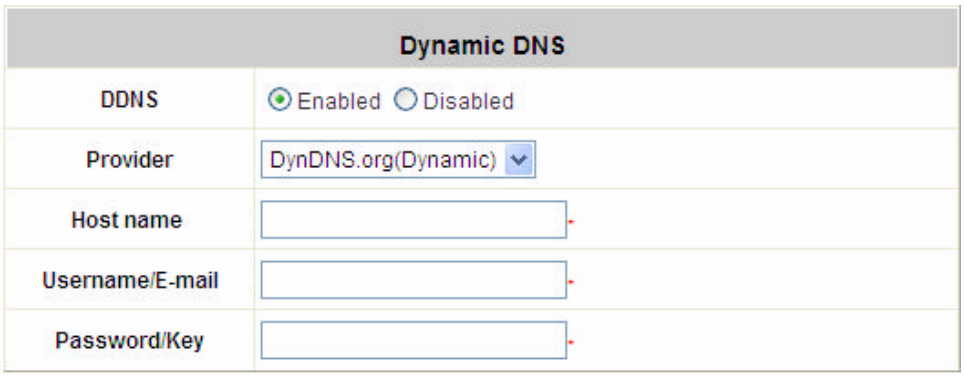
External Proxy Server		
Item	Server IP	Port
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Internal Proxy Server	
Built-in Proxy Server	○ Enabled ◉ Disabled

- **External Proxy Server:** Under the WMS-208 security management, the system will match the External Proxy Server list to the end-users' proxy setting. If there isn't a matching, then the end-users will **not** be able to reach the login page and thus unable to access the network. If there is a matching, then the end-users will be directed to the system first for authentication. After a successful authentication, the end-users will be redirected back to the desired proxy servers depending on various situations.
- **Internal Proxy Server:** WMS-208 has a built-in proxy server. If this function is enabled, the end users will be forced to treat WMS-208 as the proxy server regardless of the end-users' original proxy settings.

4.4.6 Dynamic DNS

WMS-208 provides a convenient DNS function to translate a domain name to the IP address of WAN port that helps the administrator memorize and connect to WAN port. If the DHCP is activated at WAN port, this function will also update the newest IP address regularly to the DNS server. These settings will become effective immediately after clicking ***Apply***.



- **DDNS:** Enabling or disabling of this function.
- **Provider:** Select a DNS provider.
- **Host name:** The IP address/domain name of the WAN port.
- **Username/E-mail:** The register ID (username or e-mail) for the DNS provider.
- **Password/Key:** The register password for the DNS provider.

4.4.7 IP Mobility

WMS-208 supports IP PNP function.

IP Mobility	
IP PNP	◉ Enable ○ Disable

At the user end, a static IP address can be used to connect to the system. Regardless of what the IP address at the user end is, authentication can still be performed through WMS-208.

4.4.8 VPN Configuration

***V**irtual **P**rivate **N**etwork*, or **VPN**, a type of technology designed to increase the security of information transferred over the Internet. VPN can work with either wired or wireless networks, as well as with dial-up connections over POTS. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate servers and database.

PheeNet WMS-208 provides 3 types of VPN for different network usage scenarios. Here we'll use local VPN as an example.

VPN Configuration
Local VPN
Remote VPN
Site-to-Site VPN

- **Local VPN**

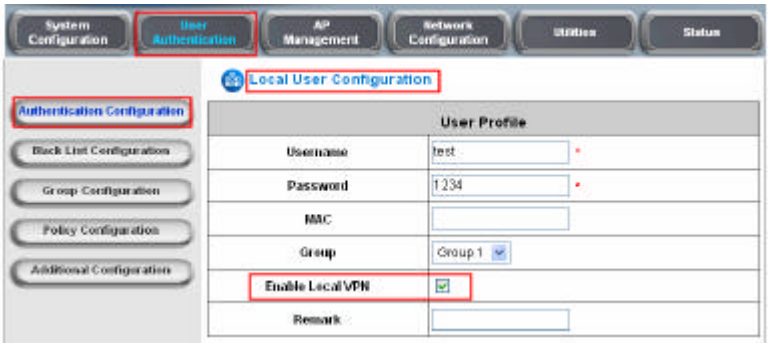
Local VPN allows users to create the VPN tunnel between a user's device and WMS-208, to encrypt wired and wireless data transmission. In addition, only when this function is enabled (***Active***) here do users of the entire system are able to use Local VPN. Local VPN users can also be isolated from each other when ***VPN Client Isolation*** is enabled.

Local VPN For The Entire System	
Active	◉ Enable ○ Disable
VPN Client Isolation	○ Enable ◉ Disable

IPSec Parameters	
Encryption	○ DES ◉ 3-DES
Integrity	◉ MD5 ○ SHA-1
Diffie-Hellman	◉ Group 1 ○ Group 2

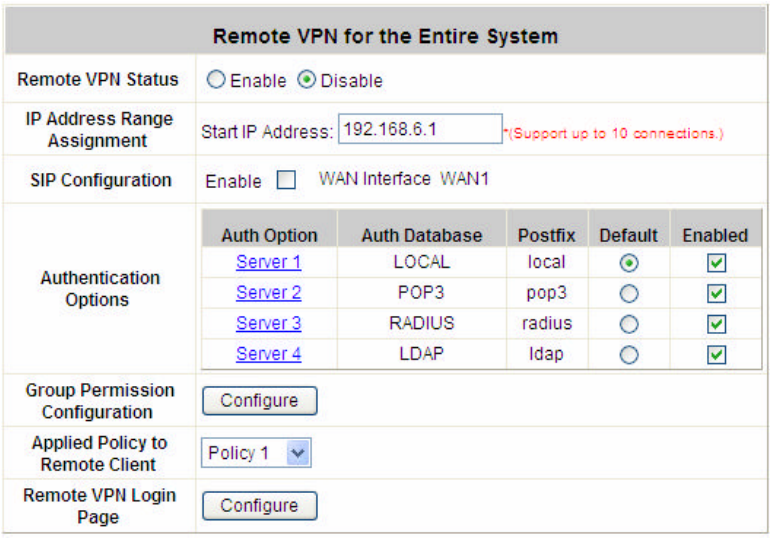
For more information about Local VPN, please see ***Appendix H. Local VPN***.

Note: *When users are required to use Local VPN for data security, their user accounts have to be configured properly to do so. For example, when adding a user account (user1) into the* ***Local*** *user database, administrator should check the "****Local VPN****" box:*



- **Remote VPN**

When the setting is enabled, the system allows the VPN tunnel between a remote client and the system to encrypt the data transmission via PPTP. The system's VPN supports end-users' device under Windows 2000, Windows XP SP1, SP2 and Windows Vista. Start IP field must be entered when enabled. The supported Authentication Servers, Group Permission, Client Policy, and the Remote VPN login page also can be configured here. The system supports up to 10 PPTP connections.



- **Site-to-Site VPN**

Enable Site-to-Site VPN can create the IPSec VPN tunnel between two remote networks/sites to encrypt the data transmission. Click ***Add A New Site Entry*** button to set configuration about remote VPN capable devices such as a VPN gateway. Click ***Add A Local Entry*** button to set configuration about local site.

Remote Site Configuration

Name	IP Address	Pre-shared Key	Edit	Delete
TPE	1.2.3.4	12345	Edit	Delete
BJ	2.3.4.5	1111	Edit	Delete

Add A Remote Site

Local Site Configuration

Local Subnet	Local Interface	Remote VPN Gateway	Remote Subnet	Edit	Delete
192.168.1.0/24	WAN1	1.2.3.4	192.168.11.0/24	Edit	Delete
192.168.2.0	WAN1	2.3.4.5	192.168.4.0/24	Edit	Delete

Add A Local Site

Click ***Add A Remote Site*** to enter the **Remote VPN Gateway** page for further configuration.

Remote VPN Gateway

Name	
IP Address	
Authentication Method	Pre-shared Key
Pre-shared Key	
Phase1 Proposal	Encryption AES256 Authentication SHA-1
Diffie-Hellman Group	Group 1 Group 2 Group 5
IKE Life Time	IKE Life Time 8h (s: second, m: minute, h: hour, d: day)
Dead Peer Detection	DPD Delay 10 (second) DPD Timeout 15 (second)

Remote Subnet

No.	Network	Mask
1		255.255.255.255 (/32)
2		255.255.255.255 (/32)
3		255.255.255.255 (/32)
4		255.255.255.255 (/32)
5		255.255.255.255 (/32)

Click ***Add A Local Site*** to enter the **Site Information** page for further configuration of local site.

Site Information	
Local Interface	WAN1
Remote Gateway IP Address	EDIT NEW
Local Subnet	(in prefix notation: x.x.x.x/yy)
Remote Subnet	
Phase2 Proposal	Encryption AES256 Authentication SHA-1
Key Life Time	Key Life Time 24h (s:second, m:minute, h:hour, d:day)
Rekey	Enable Rekey Rekey Margin 9m (second)
Perfect Forward Secrecy	Enable PFS PFS GroupMODP1024 Group 2

Click ***NEW*** to enter the screen of **Remote VPN Gateway**.

Remote VPN Gateway	
Name	
IP Address	
Authentication Method	Pre-shared Key
Pre-shared Key	
Phase1 Proposal	Encryption AES256 Authentication SHA-1
Diffie-Hellman Group	Group 1 Group 2 Group 5
IKE Life Time	IKE Life Time 8h (s: second, m: minute, h: hour, d: day)
Dead Peer Detection	DPD Delay 10 (second) DPD Timeout 15 (second)

Remote Subnet		
No.	Network	Mask
1		255.255.255.255 (/32)
2		255.255.255.255 (/32)
3		255.255.255.255 (/32)
4		255.255.255.255 (/32)
5		255.255.255.255 (/32)

4.5 Utilities

This section provides four utilities to customize and maintain the system including **Change Password**, **Backup/Restore Settings**, **Firmware Upgrade**, **Restart** and **Network Utilities**.

4.5.1 Change Password

WMS-208 supports three accounts with different access privileges. Choose to log in as **admin**, **manager** or **operator**. The default password and access privilege for each account are as follow:

Admin: The administrator can access all configuration pages of the WMS-208.

User Name: **admin**

Password: **admin**

Manager: The manager can only access the configuration pages under ***User Authentication*** to manage the user accounts, but has no permission to change the settings of the profiles for Firewall, Specific Route and Schedule.

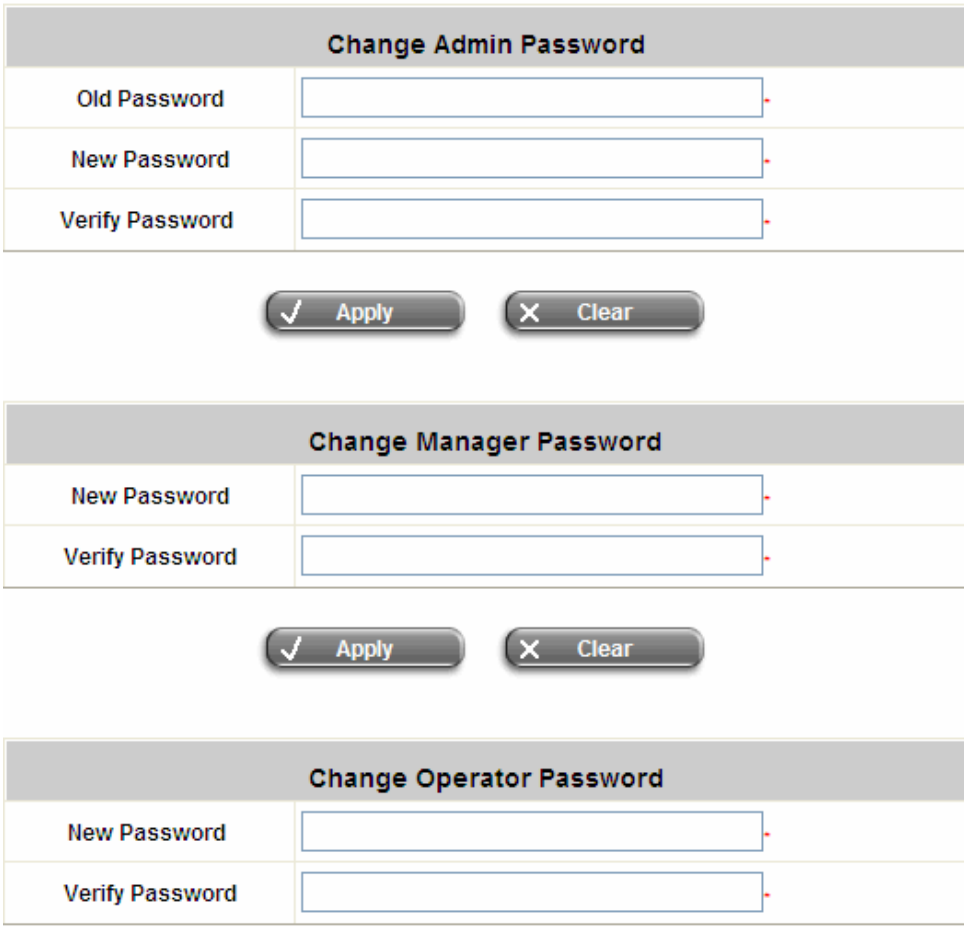
User Name: **manager**

Password: **manager**

Operator: The operator can only access the configuration page of ***Create On-demand User*** to create and print out the new on-demand user accounts.

User Name: **operator**

Password: **operator**

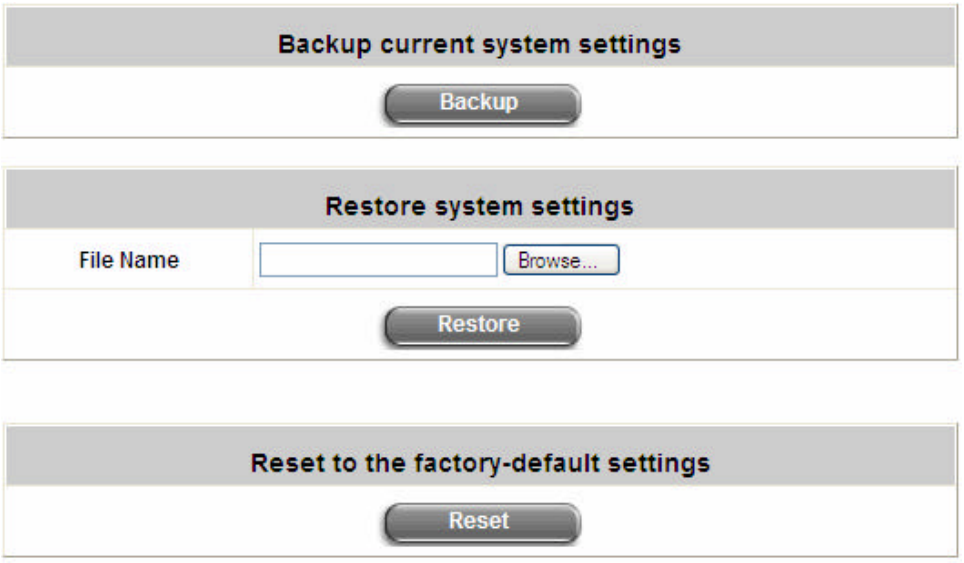


The administrator can change the passwords here. Please enter the current password and then enter the new password twice to verify. Click ***Apply*** to activate this new password.

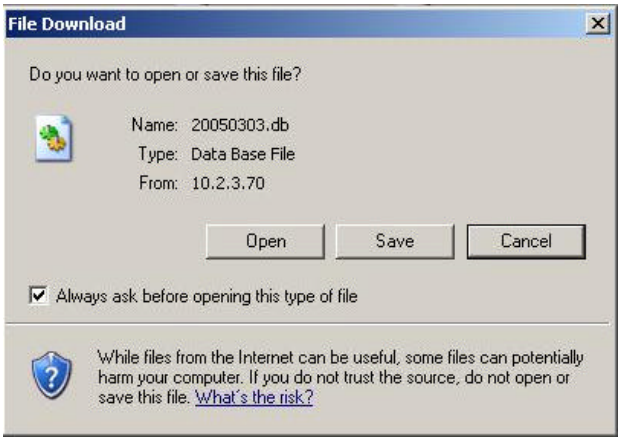
Caution: *If the administrator's password is lost, the administrator's password still can be changed through the text mode management interface on the serial port, console/printer port.*

4.5.2 Backup/Restore Setting

This function is used to backup/restore the WMS-208 settings. Also, WMS-208 can be restored to the factory default settings here.



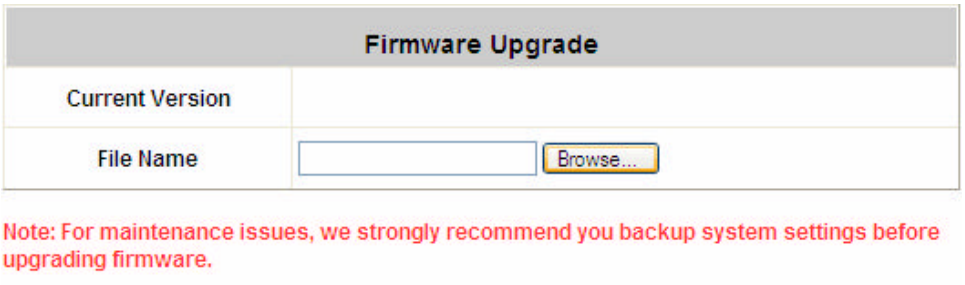
- **Backup current system setting:** Click ***Backup*** to create a .db database backup file and save it on disk.


File Download
Do you want to open or save this file?
Name: 20050303.db
Type: Data Base File
From: 10.2.3.70
Open
Save
Cancel
Always ask before opening this type of file
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

- **Restore system setting:** Click ***Browse*** to search for a .db database backup file created by WMS-208 and click ***Restore*** to restore to the same settings at the time the backup file was created.
- **Reset to the factory-default settings:** Click ***Reset*** to load the factory default settings of WMS-208.

4.5.3 Firmware Upgrade

The administrator can download the latest firmware and upgrade the system here. Click ***Browse*** to search for the firmware file and click ***Apply*** to process firmware upgrade. It might be a few minutes before the upgrade process completes and the system needs to be restarted to make the new firmware effective.

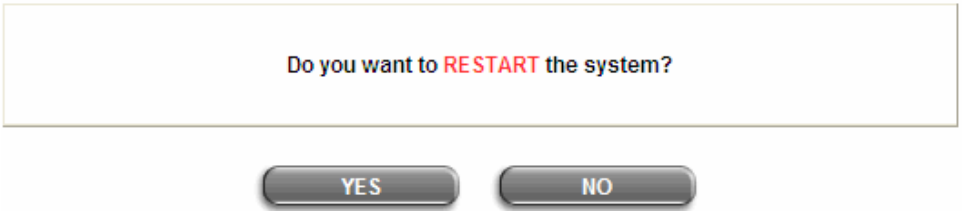

Firmware Upgrade
Current Version
File Name
Browse...
Note: For maintenance issues, we strongly recommend you backup system settings before upgrading firmware.

Warning: *1. Firmware upgrade may cause the loss of some of the data. Please refer to the release notes for the limitation before upgrading the firmware.*

2. Please restart the system after upgrading the firmware. Do not power on/off the system during the upgrade or the restart process. It may damage the system and cause it to malfunction.

4.5.4 Restart

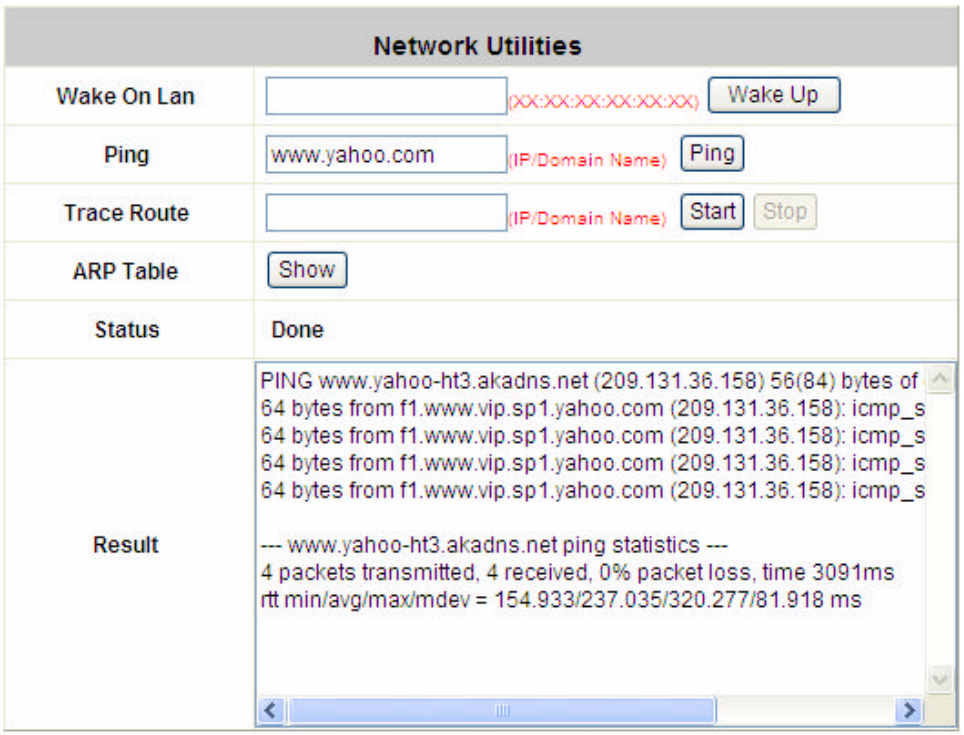
This function allows the administrator to safely restart WMS-208 and the process should take about 100 seconds. Click ***YES*** to restart WMS-208; click ***NO*** to go back to the previous screen. If turning off the power is necessary, it is recommended to restart WMS-208 first and then turn off the power after completing the restart process.



Caution: *The connection of all online users of the system will be disconnected when system is in the process of restarting.*

4.5.5 Network Utilities

This function allows the administrators to manage functions including **Wake-on-LAN**, **Ping**, **Trace Route**, and showing **ARP Table** by entering IP or Domain Name.



- **Wake on LAN:** It allows the system to remotely boot up a power-down computer with Wake-On-LAN feature enabled and is on the LAN side. Enter the MAC Address of the desired device and click Wake Up button to execute this function.
- **Ping:** It allows administrator to detect a device using IP address or Host domain name to see if it is alive or not.
- **Trace Route:** It allows administrator to find out the real path of packets from the gateway to a destination using IP address or Host domain name.
- **ARP Table:** It allows administrator to view the IP-to-Physical address translation tables used by address resolution protocol (ARP).

4.6 Status

This section includes **System Status**, **Interface Status**, **Routing Table**, **Current Users**, **Traffic History**, and **Notification Configuration** to provide system status information and online user status.

Network Access Control
www.pheenet.com
Logout
Help
System Configuration
User Authentication
AP Management
Network Configuration
Utilities
Status
System Status
Interface Status
Routing Table
Current Users
Traffic History
Notification Configuration
Status
Status
System Status
Display current system settings.
Interface Status
Display the current settings of all network interfaces such as WAN and service zone.
Routing Table
List all Policy Route rules and Global Policy Route rules. The System Route rules are shown here as well. The Policy Route rule has higher priority than the Global Policy route rule. The System Route rule has the lowest priority.
Current Users
Display online user information including: Username, IP, MAC, packet count, byte count and idle time. Administrator may also kick out any on-line user from here.
Traffic History
Display detail usage information by day. A minimum of 3 days of history can be logged in the system.
Notification Configuration
The system can send various reports via up to 3 email accounts such as Monitor IP report, Users log, and Session Log. The external SYSLOG server and FTP server are configured here.

4.6.1 System Status

This section provides an overview of the system for the administrator.

System Status		
Current Firmware Version		3.12.00-EN-N
Build		00200
System Name		PheeNet WMS-208
Home Page		http://www.pheenet.com/
SYSLOG server - Traffic History		N/A:N/A
SYSLOG server - On-demand Users Log		N/A:N/A
Proxy Server		Disabled
Warning of Internet Disconnection		Disabled
WAN Failover		Disabled
Load Balancing		Disabled
SNMP		Disabled
History	Retained Days	3 days
	Email To	N/A
		N/A
		N/A
Time	NTP Server	tock.usno.navy.mil
	Date Time	2008/05/27 17:22:14 +0800
User	Idle Timer	10 Min(s)
	Multiple Login	Disabled
DNS	Preferred DNS Server	208.67.222.222
	Alternate DNS Server	N/A

The description of the table is as follows:

Item		***Description***
Current Firmware Version		The present firmware version of WMS-208
Build		The current build number.
System Name		The system name. The default is WMS-208
Home Page		The page the users are directed to after initial login success.
Syslog server-Traffic History		The IP address and port number of the external Syslog Server. **N/A** means that it is not configured.
Syslog server-On demand User log		The IP address and port number of the external Syslog Server. **N/A** means that it is not configured.
Proxy Server		Enabled/disabled stands for that the system is currently using the proxy server or not.
Warning of Internet Disconnection		Enabled/Disabled stands for the connection at WAN is normal or abnormal (**Internet Connection Detection**) and all online users are allowed/disallowed to log in the network.
WAN Failover		Enabled/Disabled stands for the function currently being used or not.
Load Balancing		Enabled/Disabled stands for the function currently being used or not.
SNMP		Enabled/disabled stands for the current status of the SNMP management function.
History	**Retained Days**	The maximum number of days for the system to retain the users' information.
	Email To	The email address to which the traffic history or user's traffic history information will be sent.
Time	**NTP Server**	The network time server that the system is set to align.
	Date Time	The system time is shown as the local time.
User	**Idle Timer**	The minutes allowed for the users to be inactive before their account expires automatically.
	Multiple Login	Enabled/disabled stands for the current setting to allow/disallow multiple logins form the same account.
DNS	**Preferred DNS Server**	IP address of the preferred DNS Server.
	Alternate DNS Server	IP address of the alternate DNS Server.

4.6.2 Interface Status

This section provides an overview of the interface for the administrator including **WAN1**, **WAN2**, **SZ default~8**.

Interface Status		
WAN1	MAC Address	
	IP Address	
	Subnet Mask	255.255.255.0
WAN2	Disabled	
	WAN1	WAN2
Packets In	275016 (Δ 183502)	0 (Δ 0)
Packets Out	49083 (Δ 29436)	0 (Δ 0)
Bytes In	42071842 (Δ 18818367)	0 (Δ 0)
Bytes Out	12234635 (Δ 9642600)	0 (Δ 0)
Service Zone - Default	Mode	NAT
	MAC Address	00:11:A3:08:36:B6
	IP Address	192.168.10.254
	Subnet Mask	255.255.255.0
Service Zone - Default DHCP Server	Status	Enabled
	WINS IP Address	N/A
	Start IP Address	192.168.10.1
	End IP Address	192.168.10.100
	Lease Time	1440 Min(s)
Service Zone - SZ1	Disabled	

The description of the table is as follows.

Item		***Description***
WAN1	**MAC Address**	The MAC address of the WAN1 port.
	IP Address	The IP address of the WAN1 port.
	Subnet Mask	The Subnet Mask of the WAN1 port.
WAN2	**MAC Address**	The MAC address of the WAN2 port.
	IP Address	The IP address of the WAN2 port.
	Subnet Mask	The Subnet Mask of the WAN2 port.
Packets In		The total accumulated packets in through this WAN port since the gateway boots up. The delta shows the difference between the numbers from last time this Interface Status page is visited.
Packets Out		The total accumulated packets out through this WAN port since the gateway boots up. The delta shows the difference between the numbers from last time this Interface Status page is visited.
Bytes In		The total accumulated bytes in through this WAN port since the gateway boots up. The delta shows the difference between the numbers from last time this Interface Status page is visited.
Bytes Out		The total accumulated packets out through this WAN port since the gateway boots up. The delta shows the difference between the numbers from last time this Interface Status page is visited.
Service Zone - Default DHCP Server	**Status**	Enable/disable stands for status of the DHCP server in Default Service Zone
	WINS IP Address	The WINS server IP on DHCP server. **N/A** means that it is not configured.
	Start IP Address	The start IP address of the DHCP IP range.
	End IP address	The end IP address of the DHCP IP range.
	Lease Time	Minutes of the lease time of the IP address.
Service Zone – Default	**Mode**	The operation mode of the default SZ.
	MAC Address	The MAC address of the default SZ.
	IP Address	The IP address of the default SZ.
	Subnet Mask	The Subnet Mask of the default SZ.

4.6.3 Routing Table

All the **Policy** Route rules and **Global Policy** Route rules will be listed here. Also it will show the **System** Route rules specified by each interface.

Policy 1			
Destination	Subnet Mask	Gateway	Interface

Policy 2			
Destination	Subnet Mask	Gateway	Interface

Policy 3			
Destination	Subnet Mask	Gateway	Interface

Policy 4			
Destination	Subnet Mask	Gateway	Interface

Policy 5			
Destination	Subnet Mask	Gateway	Interface

Policy 6			
Destination	Subnet Mask	Gateway	Interface

Policy 7			
Destination	Subnet Mask	Gateway	Interface

Policy 8			
Destination	Subnet Mask	Gateway	Interface

Policy 9			
Destination	Subnet Mask	Gateway	Interface

Policy 10			
Destination	Subnet Mask	Gateway	Interface

Policy 11			
Destination	Subnet Mask	Gateway	Interface

Policy 12			
Destination	Subnet Mask	Gateway	Interface

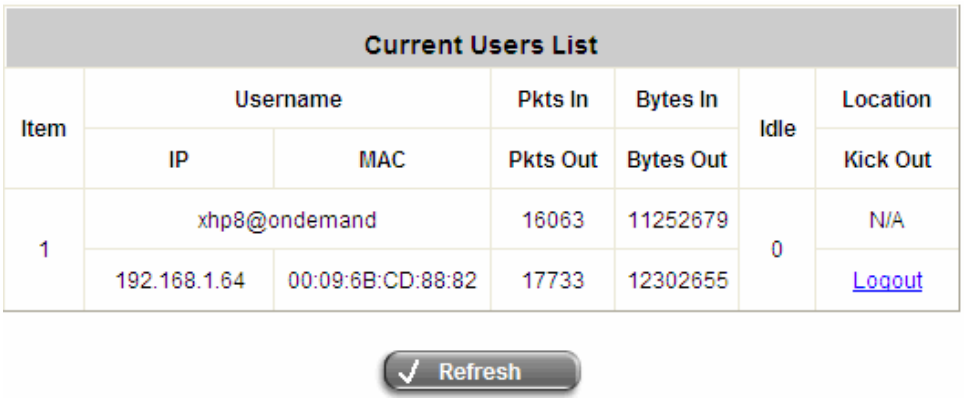
Global Policy			
Destination	Subnet Mask	Gateway	Interface

System			
Destination	Subnet Mask	Gateway	Interface
192.168.2.0	255.255.255.0	0.0.0.0	SZ1
192.168.1.0	255.255.255.0	0.0.0.0	Default
10.29.0.0	255.255.0.0	0.0.0.0	WAN1
0.0.0.0	0.0.0.0	10.29.0.1	WAN1

- **Policy 1~12:** Shows the information of the individual Policy from 1 to 12.
- **Global Policy:** Shows the information of the Global Policy.
- **System:** Shows the information of the system administration.
  - **Destination:** The destination IP address of the device.
  - **Subnet Mask:** The Subnet Mask IP address of the port.
  - **Gateway**: The Gateway IP address of the port.
  - **Interface:** The choice of interface network, including **WAN1**, **WAN2**, **Default**, or the named **Service Zones** to be applied for the traffic interface.

4.6.4 Current Users

In this function, each online user's information including **Username**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out**, **Bytes Out**, **Idle**, **Location** and **Kick Out** will be shown. Administrators can force out a specific online user by clicking the hyperlink of ***"Logout"*** and check the user access AP status by clicking the hyperlink of the AP name for "**Location**." Click ***Refresh*** is to update the current users list.



Current Users List

Item	Username		Pkts In	Bytes In	Idle	Location
	IP	MAC	Pkts Out	Bytes Out		Kick Out
1	xhp8@ondemand		16063	11252679	0	N/A
	192.168.1.64	00:09:6B:CD:88:82	17733	12302655		Logout

Refresh

4.6.5 Traffic History

This function is used to check the history of WMS-208. The history of each day will be saved separately in the DRAM for 3 days. Sorted by time, the traffic history provides all login and logout activity of specific date. Other information includes User Name, IP address, MAC address, In-bound Packet Count, Out-bound Packet Count, In-bound Byte Count, and out-bound Byte Count.

Traffic History	
Date	Size (Byte)
2007-11-22	65

On-demand User Log	
Date	Size (Byte)
2007-11-22	362

Roaming Out Traffic History	
Date	Size (Byte)
2007-11-22	106

Roaming In Traffic History	
Date	Size (Byte)
2007-11-22	112

SIP Call Usage Log	
Date	Call Count
2007-11-22	0

Monthly Network Usage of Local User		
Month	No. of Entries	Usage Data
2007-11	2	Download

Caution: *Since the history is saved in the DRAM, if you need to restart the system and also keep the history, please manually copy and save the information before restarting.*

If the **History Email** has been entered under the **Notification Configuration** page, the system will automatically send out the history information to that email address.

- **Traffic History**

  As shown in the following figure, each line is a traffic history record consisting of 9 fields, **Date**, **Type, Name**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out,** and **Bytes Out**, of user activities.

Traffic History 2005-03-22

Date	Type	Name	IP	MAC	Pkts In	Bytes In	Pkts Out	Bytes Out
2005-03-22 19:12:21 +0800	LOGIN	user1@local.tw	192.168.1.143	00:D0:C9:42:37:20	0	0	0	0
2005-03-22 19:12:24 +0800	LOGOUT	user1@local.tw	192.168.1.143	00:D0:C9:42:37:20	3	252	3	252
2005-03-22 19:12:29 +0800	LOGIN	user2@local.tw	192.168.1.143	00:D0:C9:42:37:20	0	0	0	0
2005-03-22 19:12:32 +0800	LOGOUT	user2@local.tw	192.168.1.143	00:D0:C9:42:37:20	3	252	3	252
2005-03-22 19:13:51 +0800	LOGIN	user1@local.tw	192.168.1.1	00:D0:C9:60:01:01	0	0	0	0

- **On-demand User Log**

  As shown in the following figure, each line is a on-demand user log record consisting of 13 fields, **Date**, **System Name**, **Type**, **Name**, **IP**, **MAC**, **Pkts In**, **Bytes In**, **Pkts Out, Bytes Out, 1st Login Expiration Time**, **Account Valid Through** and **Remark**, of user activities.

On-demand User Log 2007-11-26

Date	System Name	Type	Name	IP	MAC	Pkts In	Bytes In	Pkts Out	Bytes Out	1st Login Expiration Time	Account Valid Through	Remark
2007-11-26 14:58:04	AirLive MV-2000S	Create_OD_User	8s3g	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2007-11-28 02:58:03	None	Plan 1
2007-11-26 14:58:10	AirLive MV-2000S	Create_OD_User	u96u	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2007-11-28 14:58:10	None	Plan 2
2007-11-26 14:58:15	AirLive MV-2000S	Create_OD_User	n4ka	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2007-11-28 14:58:15	None	Plan 3
2007-11-26 14:58:19	AirLive MV-2000S	Create_OD_User	bk35	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2007-11-28 02:58:19	None	Plan 4
2007-11-26 14:58:35	AirLive MV-2000S	Create_OD_User	4z4m	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2007-11-28 02:58:35	None	Plan 1
2007-11-26 14:58:40	AirLive MV-2000S	Create_OD_User	kkx5	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2007-11-28 14:58:39	None	Plan 2
2007-11-26 14:58:47	AirLive MV-2000S	Create_OD_User	6m5p	0.0.0.0	00:00:00:00:00:00	0	0	0	0	2007-11-28 02:58:47	None	Plan 4
2007-11-26 15:01:52	AirLive MV-2000S	OD_User_Login	u96u	192.168.1.64	00:09:6B:CD:88:82	0	0	0	0	None	2007-11-28 15:01:52	None
2007-11-26 15:04:21	AirLive MV-2000S	OD_User_Logout	u96u	192.168.1.64	00:09:6B:CD:88:82	85	31812	89	12350	None	2007-11-28 15:01:52	Logout
2007-11-26 15:04:51	AirLive MV-2000S	OD_User_Login	bk35	192.168.1.64	00:09:6B:CD:88:82	0	0	0	0	None	2007-11-28 15:04:51	None
2007-11-26 15:07:02	AirLive MV-2000S	OD_User_Logout	bk35	192.168.1.64	00:09:6B:CD:88:82	4	252	7	360	None	2007-11-28 15:04:51	Logout

- **Roaming Out Traffic History**

  As shown in the following figure, each line is a roaming out traffic history record consisting of 14 fields, **Date**, **Type, Name**, **NSID**, **NASIP**, **NASPort**, **UserMAC**, **SessionID**, **SessionTime**, **Bytes in**, **Bytes Out**, **Pkts In**, **Pkts Out** and **Message**, of user activities.

Roaming Out Traffic History 2005-03-22

Date	Type	Name	NASID	NASIP	NASPort	UserMAC	sessionID	sessionTime	Bytes In	Bytes Out	Pkts In	Pkts Out	Message

- **Roaming In Traffic History**

  As shown in the following figure, each line is a roaming in traffic history record consisting of 15 fields, **Date**, **Type, Name**, **NSID**, **NASIP**, **NASPort**, **UserMAC**, **UserIP**, **SessionID**, **SessionTime**, **Bytes in**, **Bytes Out**, **Pkts In**, **Pkts Out** and **Message**, of user activities.

Roaming In Traffic History 2005-03-22

Date	Type	Name	NASID	NASIP	NASPort	UserMAC	UserIP	SessionID	SessionTime	Bytes In	Bytes Out	Pkts In	Pkts Out	Message

- **SIP Call Usage Log**

  The log provides the login and logout activities of SIP clients (device and soft clients) such as Start Time, Caller, Callee and Duration (seconds)

SIP Call Usage Log			
Start Time	Caller	Callee	Duration (seconds)

- **Monthly Network Usage of Local User**

  The system will record the network usage of local users every month. In addition, the data will be stored locally for up to two months and can be exported as a text file in CSV format. As follows are the descriptions of fields in the usage record.

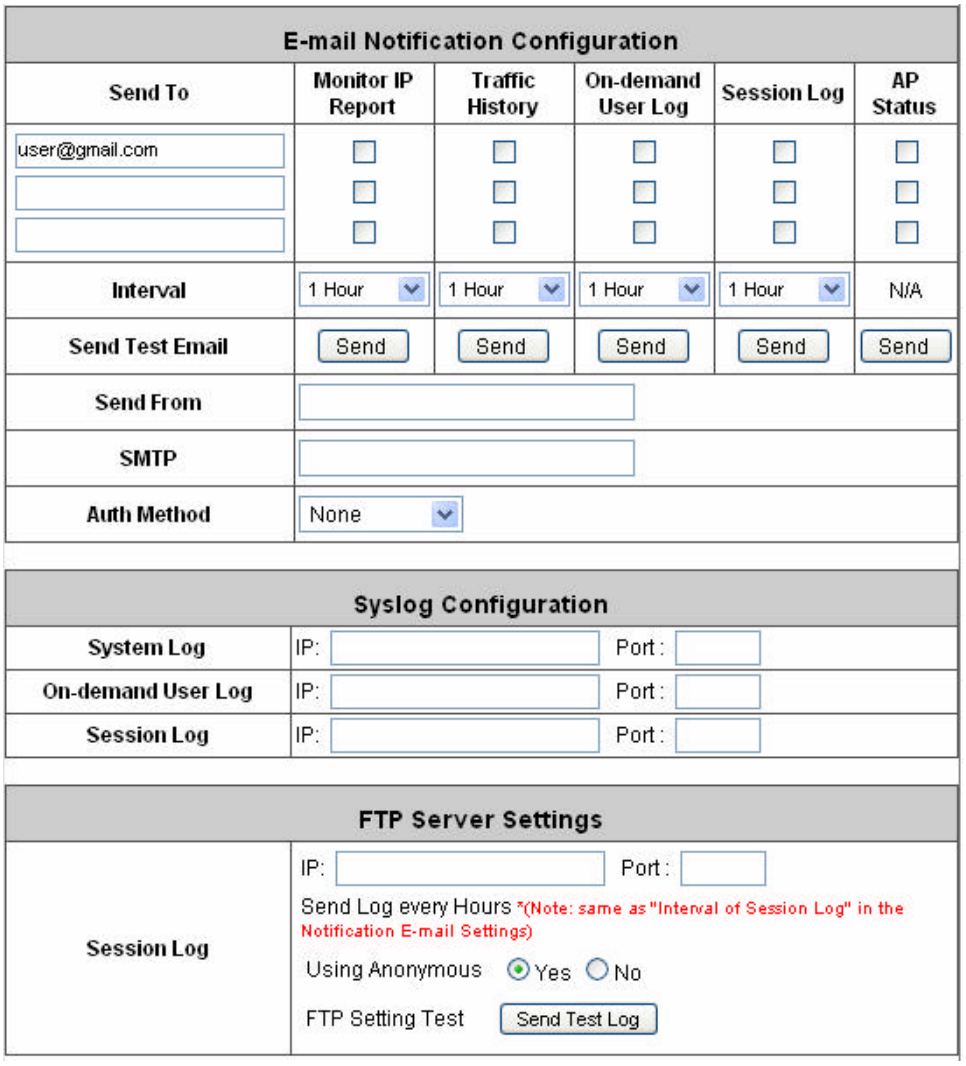
Monthly Report 2007-11					
Username	Connection Time Usage	Packets In	Bytes In	Packets Out	Bytes Out
user1	8 mins 42 secs	195	86.9K	202	23K
user2	1 min 43 secs	27K	23.1M	21.3K	12.1M

(Total: 2)
First Previous Next Last

  - **Username:** Username of the local user account.
  - **Connection Time Usage:** The total time used by the user.
  - **Pkts In/ Pkts Out:** The total number of packets received and sent by the user.
  - **Bytes In/ Bytes Out:** The total number of bytes received and sent by the user.

4.6.6 Notification Configuration

WMS-208 can automatically send the notification of **Monitor IP Report**, **Traffic History**, **On-demand User Log**, **Session Log** and **AP status** to up to 3 particular e-mail address. The notification of AP Status is triggered by the event when a managed AP becomes unreachable while the other types of emails are sent periodically in given intervals such as 1 hour. A trial email is provided by the system for validation. In addition, the system supports recording Syslog of Traffic History, On-demand User Log and Session Log via external Syslog servers. In addition, the Session Log can be sent to a specified FTP server. Enter the related information and select the desired items and then apply the settings.



- **E-mail Notification Configuration:**
  - **Send To:** Up to 3 e-mail address can be set up to receive the notification. These are the receiver's e-mail addresses. There are four kinds of notification to selection -- Monitor IP Report, Traffic History, On-demand User Log and AP Status, and check which type of notification to be sent.
  - **Interval:** The time interval to send the e-mail report.
  - **Send Test Email:** To test the settings immediately.
  - **Send From:** The e-mail address of the administrator in charge of the monitoring. This will show up as the sender's e-mail.

- **SMTP:** The IP address of the sender's SMTP server.
- **Auth Method:** The system provides four authentication methods, **Plain**, **Login**, **CRAM-MD5** and **NTLMv1**, or **"None"** to use none of the above. Depending on which authentication method selected, enter the **Account Name**, **Password** and **Domain**.
  - **NTLMv1** is not currently available for general use.
  - **Plain** and **CRAM-MD5** are standardized authentication mechanisms while **Login** and **NTLMv1** are Microsoft proprietary mechanisms. Only **Plain** and **Login** can use the UNIX login password. Netscape uses **Plain**. Outlook and Outlook express use **Login** as default, although they can be set to use **NTLMv1**.
  - Pegasus uses **CRAM-MD5** or **Login** but which method to be used can not be configured.

- **Syslog Configuration:** There are 3 types of Syslog supported: System Log, On-demand User Log, and Session Log. Enter the IP address and Port number to specify which and from where the report should be sent to.

Note: *When the number of a user's session (TCP and UDP) reaches the session limit specified in the policy, a record will be logged to this Syslog server.*

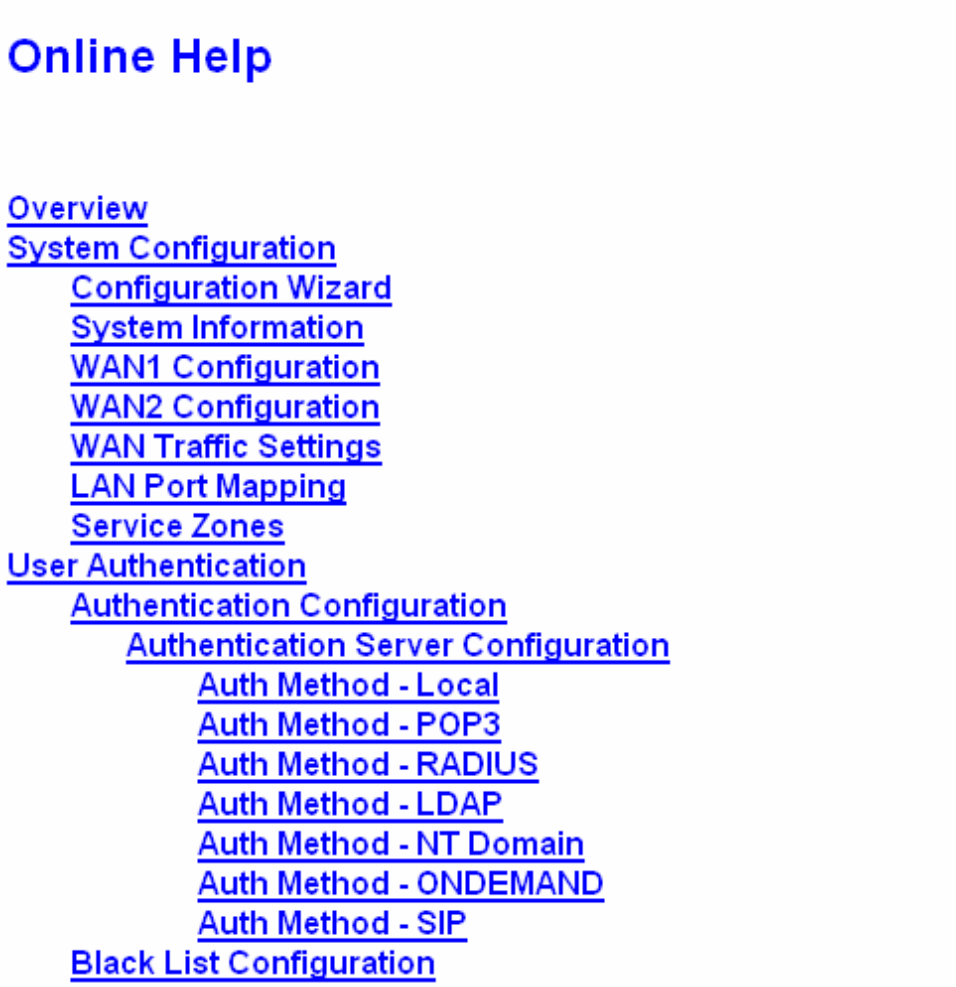
- **FTP Server Settings**

Session Log: Log each connection created by users and tracking the source IP and destination IP. If Syslog is enabled, Session Log will be sent to the Syslog server automatically during every defined interval in Session Log email notification. Session Log allows uploading the log file to a FTP server periodically. The maximum log file size is 256K. The log file will be sent to the FTP server once the file size reaches its maximum size or periodical time interval.

4.7 Help

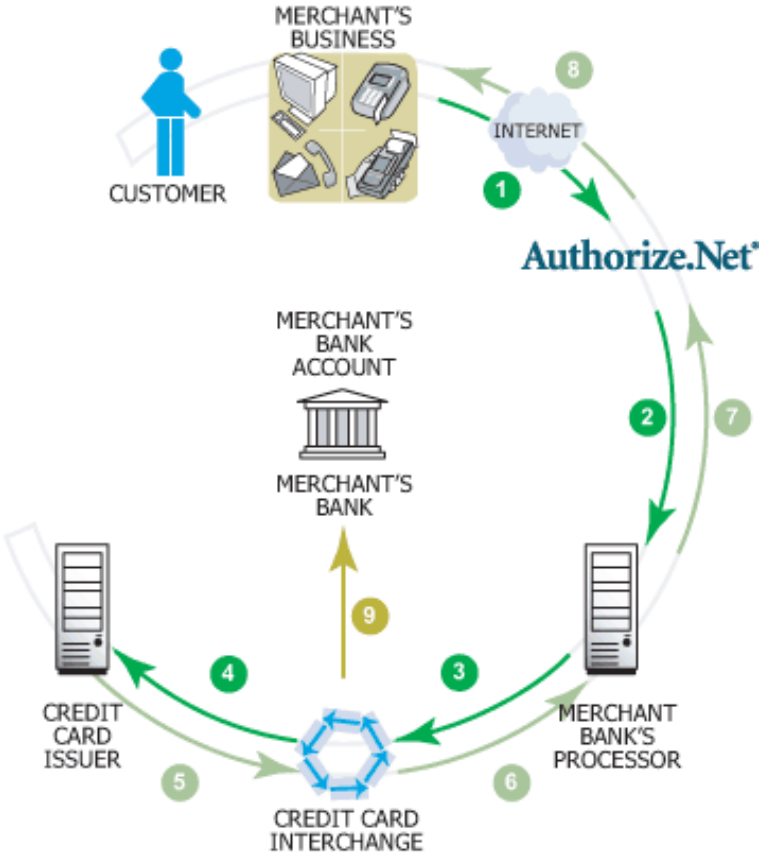
On the screen, the **Help** button is on the upper right corner.

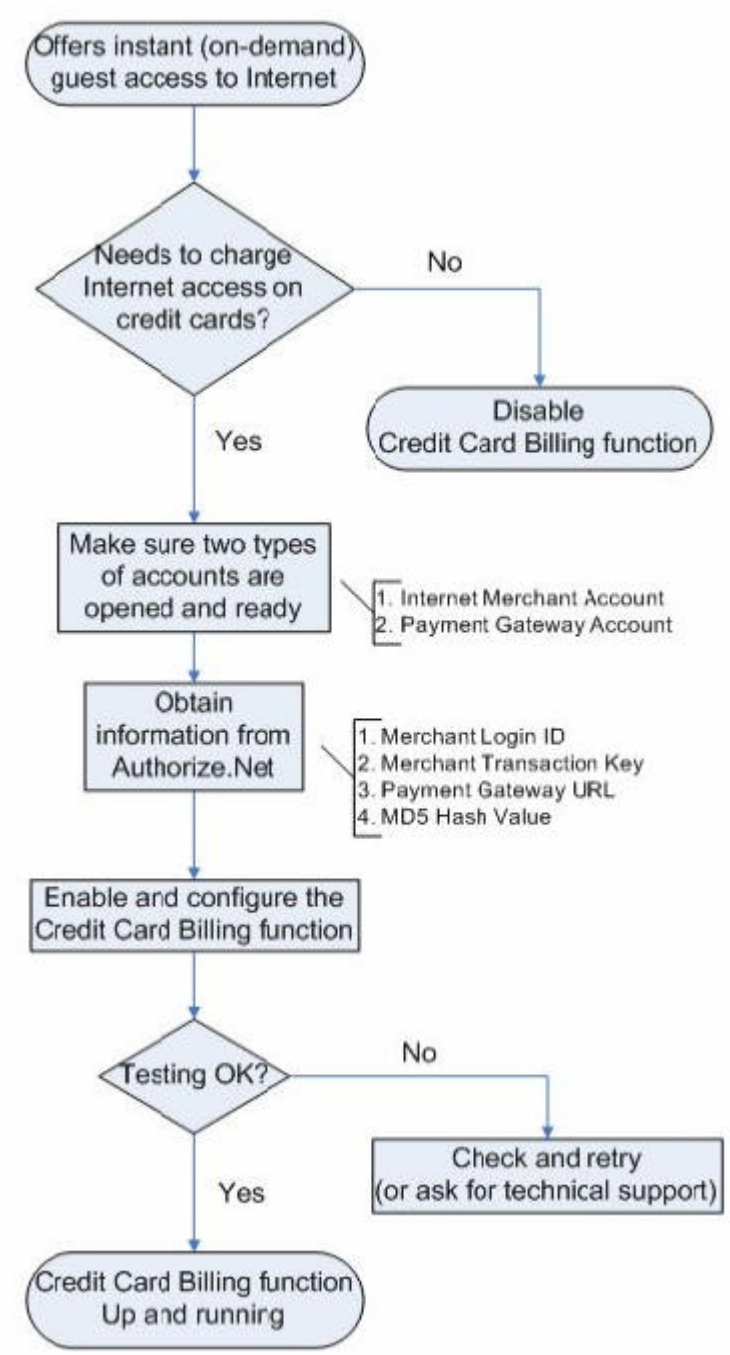
Click ***Help*** to the **Online Help** window and then click the hyperlink of the items to get the information.



Appendix A. Accepting Payment via Authorize.Net

This section is to show independent Hotspot owners how to configure related settings in order to accept credit card payments via Authorize.Net, making the Hotspot an e-commerce environment for clients to pay for and obtain Internet access using their credit cards.



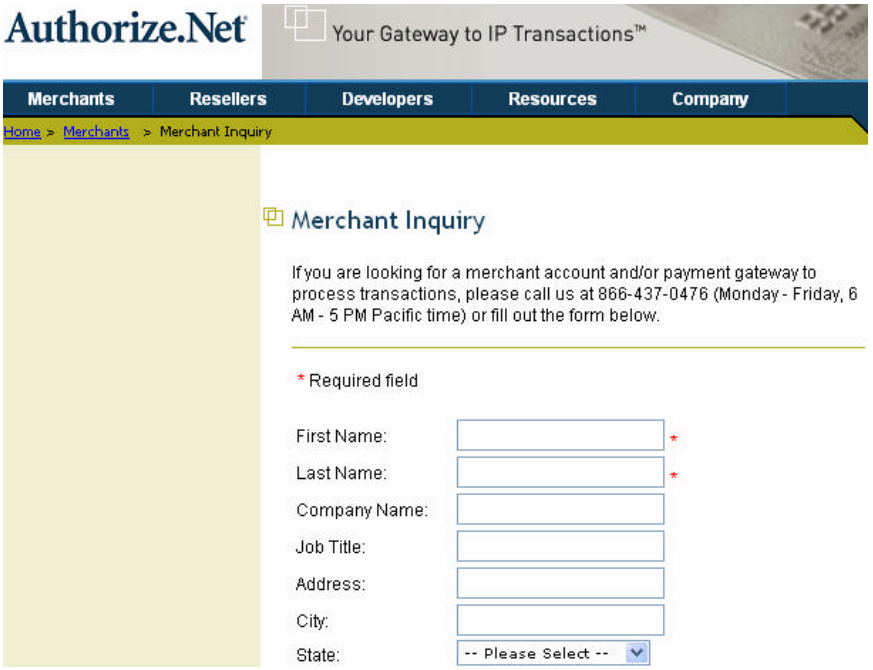

Offers instant (on-demand) guest access to Internet
Needs to charge Internet access on credit cards?
No
Disable Credit Card Billing function
Yes
Make sure two types of accounts are opened and ready
1. Internet Merchant Account
2. Payment Gateway Account
Obtain information from Authorize.Net
1. Merchant Login ID
2. Merchant Transaction Key
3. Payment Gateway URL
4. MD5 Hash Value
Enable and configure the Credit Card Billing function
Testing OK?
No
Check and retry (or ask for technical support)
Yes
Credit Card Billing function Up and runnirg

1. Setting Up

1.1 Open Accounts

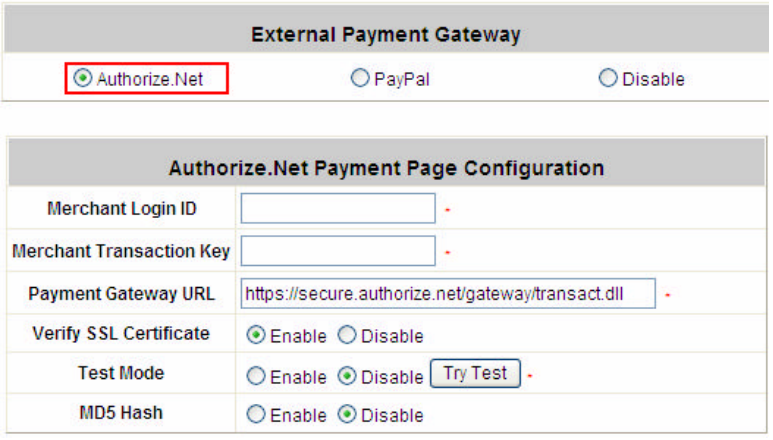
To set up PheeNet WMS-208 to process credit card billing, the merchant owner will need two accounts (Internet Merchant account and Authorize.Net account).

If you are looking for a merchant account or Internet payment gateway to process transactions, you can fill out the Inquiry Form on http://www.authorize.net/solutions/merchantsolutions/merchantinquiryform/.



1.2 Configure PheeNet WMS-208 using an Authorize.Net account

Please log in PheeNet WMS-208. **User Authentication** >> **Authentication Configuration** >> Click the server name ***On-demand User*** >> **External Payment Gateway** >> Click ***Configure*** >> **External Payment Gateway** >> Select ***Authorize.Net***



Some major fields are required:

Setting	Description
Merchant Login ID	This is the "Login ID" that comes with the Authorize.Net account.
Merchant Transaction Key	To get a new key, please log in Authorize.Net >> Click **Settings and Profile** >> Go to the **"Security"** section >> Click **Obtain Transaction Key** >> Enter **"Secret Answer"** >> Click ***Submit.***
Payment Gateway URL	https://secure.authorize.net/gateway/transact.dll (default gateway address)
MD5 Hash	To enhance the transaction security, merchant owner can choose to enable this function and enter a value in the text box: **"MD5 Hash Value"**.

Note: *For detailed description, please see* ***4.2.1.6 ONDEMAND Authentication***

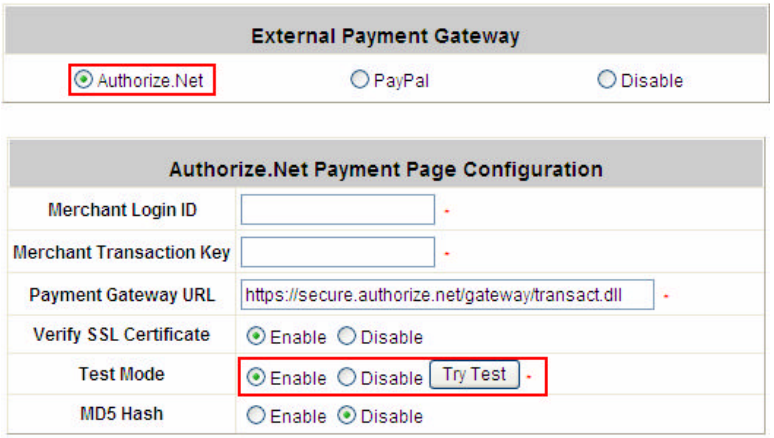
1.3 Configure the Authorize.Net Merchant Account to Match the Configuration of PheeNet WMS-208

Settings of the merchant account on Authorize.Net should be matched with the configuration of PheeNet WMS-208:

Setting	Description
MD5 Hash	To configure **"MD5 Hash Value"**, please log in Authorize.Net >> Click **Settings and Profile** >> Go to the **"Security"** section >> Click **MD5 Hash** >> Enter **"New Hash Value"** & **"Confirm Hash Value"** >> Click ***Submit***.
Required Card Code	If the **"Card Code"** is set up as a required field, please log in Authorize.Net >> Click **Settings and Profile** >> Go to the **"Security"** section >> Click **Card Code Verification** >> Check the **Does NOT Match (N)** box >> Click ***Submit***.
Required Address Fields	After setting up the required address fields on the **"Credit Card Payment Page Billing Configuration"** section of PheeNet WMS-208, the same requirements must be set on Authorize.Net. To do so, please log in Authorize.Net >> Click **Settings and Profile** >> Go to the **"Security"** section >> Click **Address Verification System (AVS)** >> Check the boxes accordingly >> Click ***Submit***.

1.4 Test The Credit Card Payment via Authorize.Net

To test the connection between PheeNet WMS-208 and Authorize.Net, please log in PheeNet WMS-208. **User Authentication** >> **Authentication Configuration** >> Click the server ***On-demand User*** >> **External Payment Gateway** >> Click ***Configure*** >> **External Payment Gateway** >> Select ***Authorize.Net*** >> Go to "**Authorize.Net Payment Page Configuration**" section >> ***Enable*** the **"Test Mode"** >> Click ***Try Test*** and follow the instructions



2. Basic Maintenance

In order to maintain the operation, merchant owners will have to manage the accounts and transactions via Authorize.Net as well as PheeNet WMS-208.

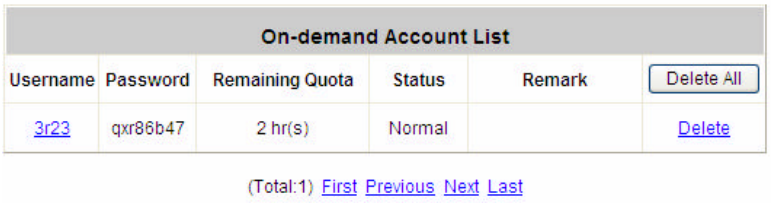
2.1 Void A Transaction and Remove the On-demand Account Generated on PheeNet WMS-208

Sometimes, a transaction (as well as the related user account on PheeNet WMS-208) may have to be canceled before it has been settled with the bank.

a. To void an unsettled transaction, please log in Authorize.Net. Click **Unsettled Transactions** >> Locate the specific transaction record on the **"List of Unsettled Transactions"** >> Click the **Trans ID** number >> Confirm and click **Void**.

Note: *To find the on-demand account name, click* ***Show Itemized Order Information*** *in the* ***"Order Information"*** *section >> Username can be found in the* ***"Item Description"***

b. To remove the specific account from PheeNet WMS-208, please log in PheeNet WMS-208. **User Authentication** >> **Authentication Configuration** >> Click the server ***On-demand User*** >> **On-demand Account List** >> Click ***View*** >> **On-demand Account List** >> Click ***Delete*** on the record with the account name. Click ***Delete All*** to delete all users at once.



2.2 Refund A Settled Transaction and Remove the On-demand Account Generated on PheeNet WMS-208

a. To refund a credit card payment, please log in Authorize.Net. Click **Virtual Terminal** >> Select a Payment Method >> Click **Refund a Credit Card** >> **Payment/Authorization Information** >> Type information in at least three fields: **Card Number**, **Expiration Date**, and **Amount** >> Confirm and click ***Submit***.

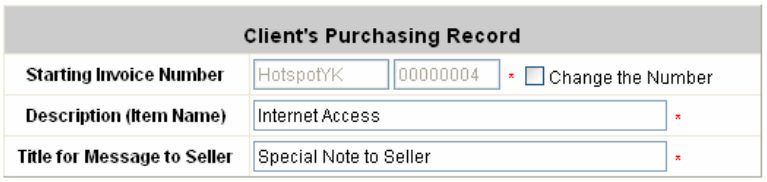
b. To remove the specific account from PheeNet WMS-208, please log in PheeNet WMS-208. **User Authentication** >> **Authentication Configuration** >> Click the server ***On-demand User*** >> **On-demand Account List** >> Click ***View*** >> **On-demand Account List** >> Click ***Delete*** on the record with the account name.

2.3 Find the Username and Password for A Specific Customer

Please log in Authorize.Net. Click **Unsettled Transactions** >> Try to locate the specific transaction record on the **"List of Unsettled Transactions"** >> Click the **Trans ID** number >> Click **Show Itemized Order Information** in the **"Order Information"** section >> Username and Password can be found in the **"Item Description"**.

2.4 Send An Email Receipt to A Customer

If a valid email address is provided, an email receipt with payment details for each successful transaction will be automatically sent to the customer via Authorize.Net. To change the information on the receipt for customer, please log in PheeNet WMS-208. **User Authentication** >> **Authentication Configuration** >> Click the server **On-demand User** >> **External Payment Gateway** >> Click ***Configure*** >> **External Payment Gateway** >> Select ***Authorize.NET*** >> Scroll down to **Client's Purchasing Record** section of the page >> Type in information in the text boxes: "**Description" and "E-mail Header"** >> Confirm and click ***Apply***.



2.5 Send an Email Receipt for Each Transaction to the Merchant Owner

A copy of email receipt with payment details for each successful transaction will also be automatically sent to the merchant owner/administrator via Authorize.Net.

To configure the contact person who will receive a receipt for each transaction, please log in Authorize.Net. Click **Settings and Profile** >> Go to the **"General"** section >> Click **Manage Contacts** >> Click **Add New Contact** to >> Enter necessary contact information on this page >> Check the **"Transaction Receipt"** box >> Click ***Submit***.

3. Reporting

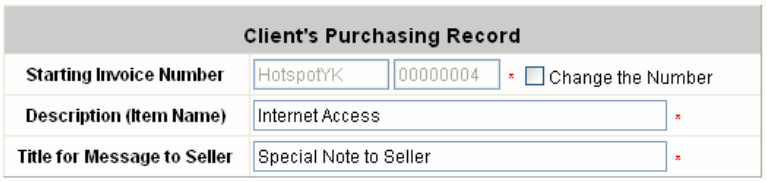
During normal operation, the following steps will be necessary to generate transaction reports.

3.1 Transaction Statistics by Credit Card Type during the Period.

Please log in Authorize.Net. >> Click **Reports** >> Check **"Statistics by Settlement Date"** radio button >> Select **"Transaction Type"**, **"Start Date"**, and **"End Date"** as the criteria >> Click ***Run Report***.

3.2 Transaction Statistics by Different Location

a. To deploy more than one PheeNet WMS-208, the way to distinguish transactions from different locations is to make the invoice numbers different. To change the invoice setting, please log in PheeNet WMS-208. **User Authentication** >> **Authentication Configuration** >> Click the server ***On-demand User*** >> **External Payment Gateway** >> Click ***Configure*** >> **External Payment Gateway** >> Select ***Authorize.NET*** >> Scroll down to **"Client's Purchasing Record"** section of the page >> Check the **"Reset"** box >> A location-specific ID (for example, Hotspot-A) can be used as the first part of **"Invoice Number"** >> Confirm and click ***Apply***.



b. Please log in Authorize.Net >> Click **Search and Download** >> Specify the transaction period (or ALL Settled, Unsettled) in **"Settlement Date"** section >> Go to **"Transaction"** section >> Enter the first part of invoice number plus an asterisk character (for example, Hotspot-A*) in the **"Invoice #"** text box >> Click ***Search*** >> If transaction records can be found, the number of accounts sold is the number of search results >> Or, click **Download To File** to download records and then use MS Excel to generate more detailed reports.

3.3 Search for The Transaction Details for A Specific Customer

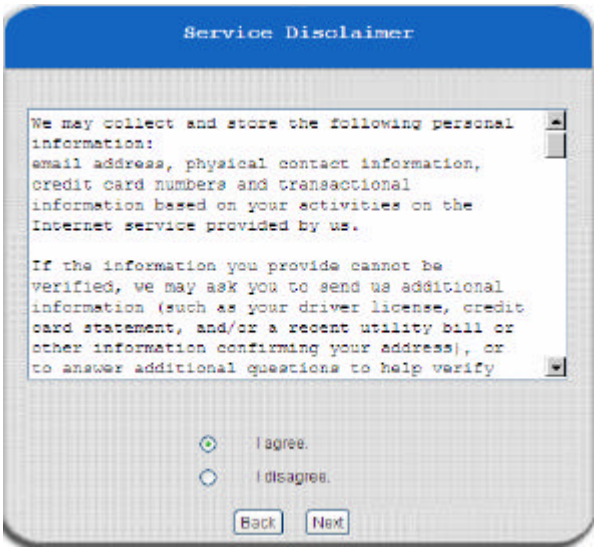
Please log in Authorize.Net. Click **Search and Download** >> Enter the information for a specific customer as criteria >> Click ***Search*** >> Click the **Trans ID** number to view the transaction details.

Note: *For more information about Authorize.Net, please see http://www.authorize.net*

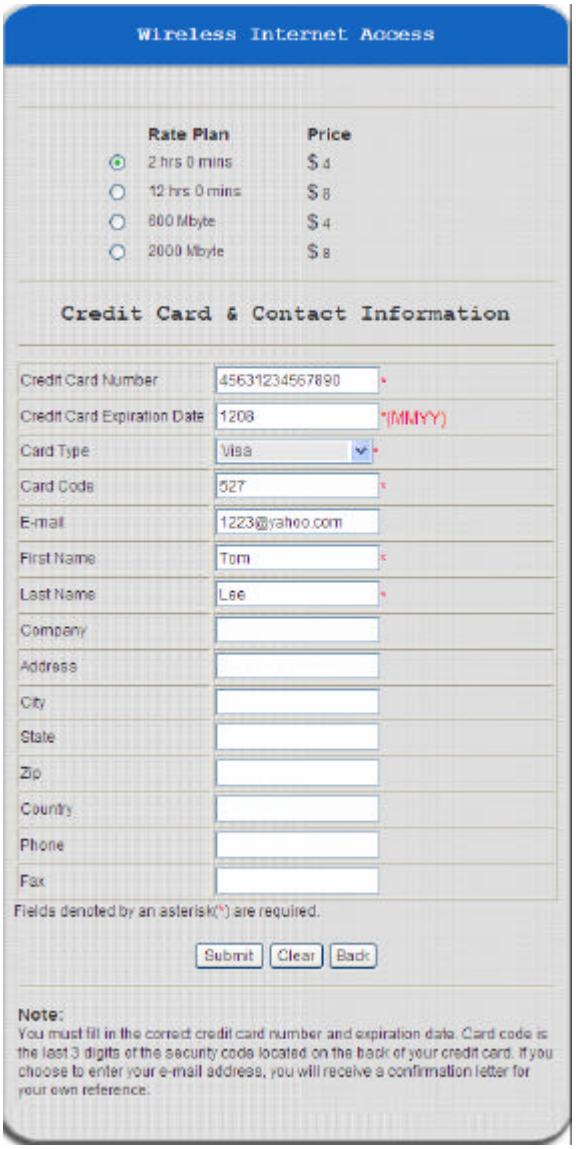
4. Examples of Making Payment for End Users

Step 1: Click the link below the login window to pay for the service by credit card via Authorize.Net.

Step 2: Choose ***I agree*** to accept the terms of use and click ***Next***.


Service Disclaimer
We may collect and store the following personal information:
email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.
If the information you provide cannot be verified, we may ask you to send us additional information (such as your driver license, credit card statement, and/or a recent utility bill or other information confirming your address), or to answer additional questions to help verify
I agree.
I disagree.
Back
Next

Step 3: Please fill out the form and Click ***Submit*** to send out this transaction. There will be a confirm dialog box.

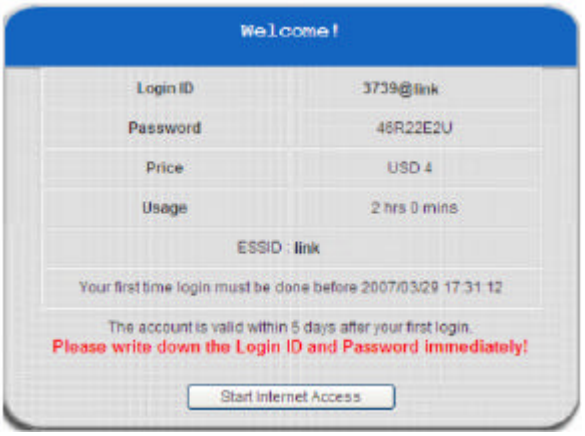


Step 4: Please confirm the data and the click ***OK*** to go on the transaction or click ***Cancel*** to revise the data or cancel this transaction. After clicking OK, there will be another dialog box showing up to confirm this transaction again.

Step 5: Click ***OK*** to complete the process or click ***Cancel*** to revise the data or cancel this transaction.

Microsoft Internet Explorer
The process may take several minnutes.
Please DO NOT close or leave this page before getting the result.
Do you want to continue the credit card payment process?
OK
Cancel

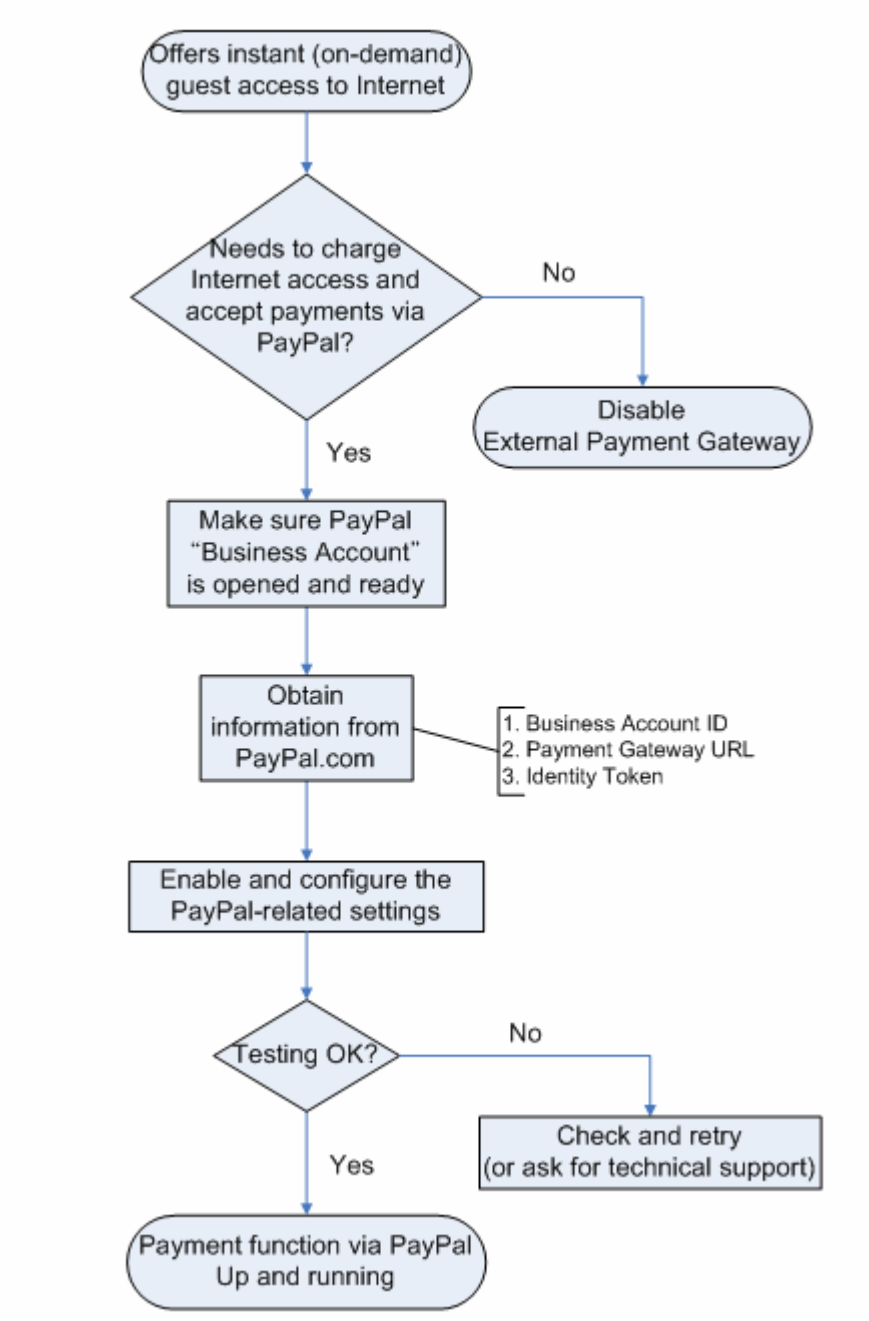
Step 6: Click ***Start Internet Access*** to use the Internet access service.



Note: *The clients must fill in the correct credit card number and expiration date. Card code is the last 3 digits of the security code located on the back of your credit card. If clients choose to enter the e-mail addresses, clients will receive confirmation letters for reference.*

Appendix B. Accepting Payment via PayPal

This section is to show independent Hotspot owners how to configure related settings in order to accept payments via PayPal, making the Hotspot an e-commerce environment for clients to pay for and obtain Internet access using their PayPal accounts or credit cards.


Offers instant (on-demand) guest access to Internet
Needs to charge Internet access and accept payments via PayPal?
No
Disable External Payment Gateway
Yes
Make sure PayPal "Business Account" is opened and ready
Obtain information from PayPal.com
1. Business Account ID
2. Payment Gateway URL
3. Identity Token
Enable and configure the PayPal-related settings
Testing OK?
No
Check and retry (or ask for technical support)
Yes
Payment function via PayPal Up and running

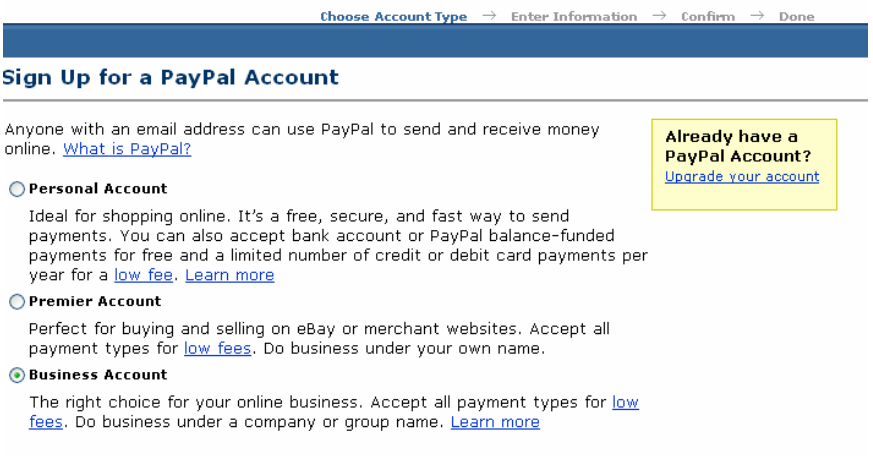
1. Setting Up

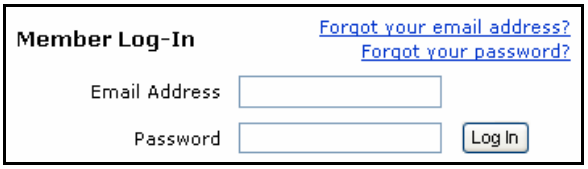
As follows are the basic steps to open and configure a "**Business Account**" on **PayPal**.

1.1 Open An Account

Step 1: Sign up for a PayPal Business Account and login.

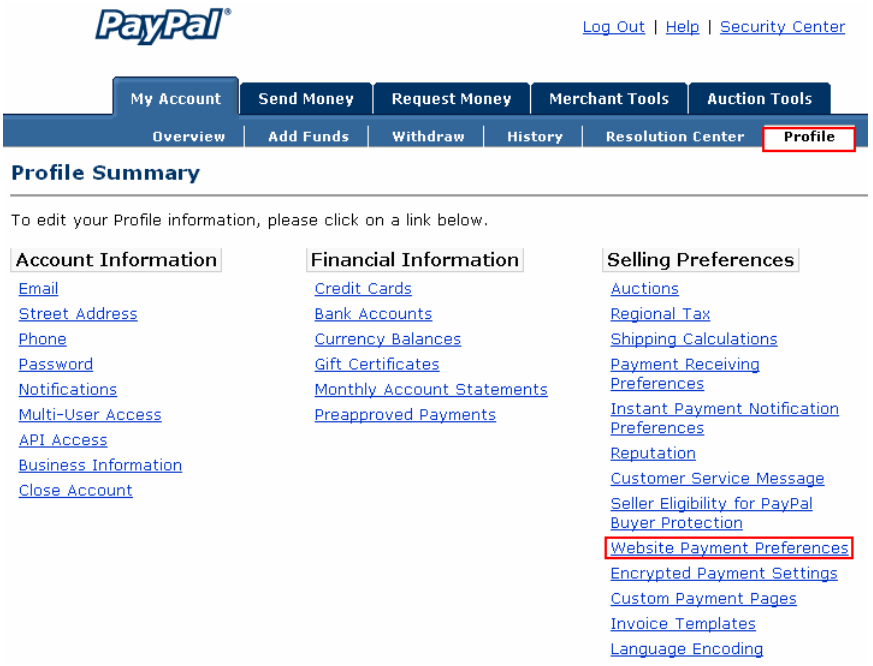
Here is a link: https://www.paypal.com/cgi-bin/webscr?cmd=_registration-run


Choose Account Type → Enter Information → Confirm → Done
Sign Up for a PayPal Account
Anyone with an email address can use PayPal to send and receive money online. What is PayPal?
Already have a PayPal Account?
Upgrade your account
Personal Account
Ideal for shopping online. It's a free, secure, and fast way to send payments. You can also accept bank account or PayPal balance-funded payments for free and a limited number of credit or debit card payments per year for a low fee. Learn more
Premier Account
Perfect for buying and selling on eBay or merchant websites. Accept all payment types for low fees. Do business under your own name.
Business Account
The right choice for your online business. Accept all payment types for low fees. Do business under a company or group name. Learn more

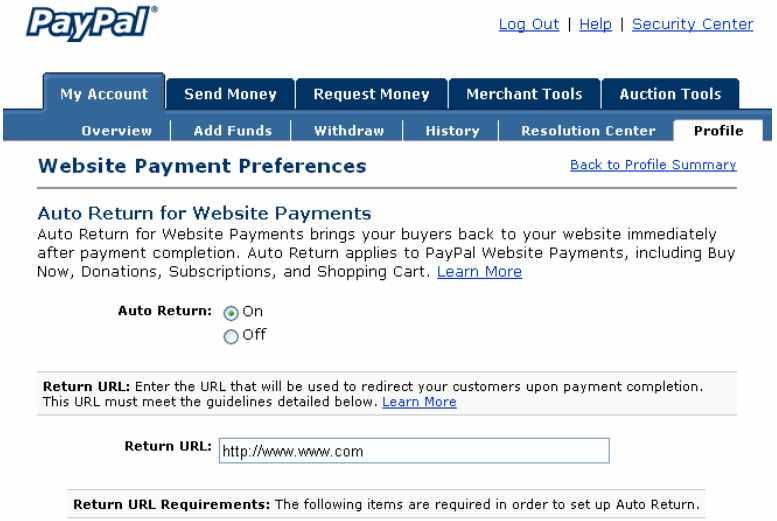
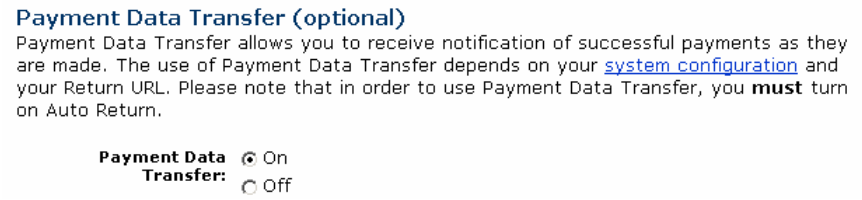
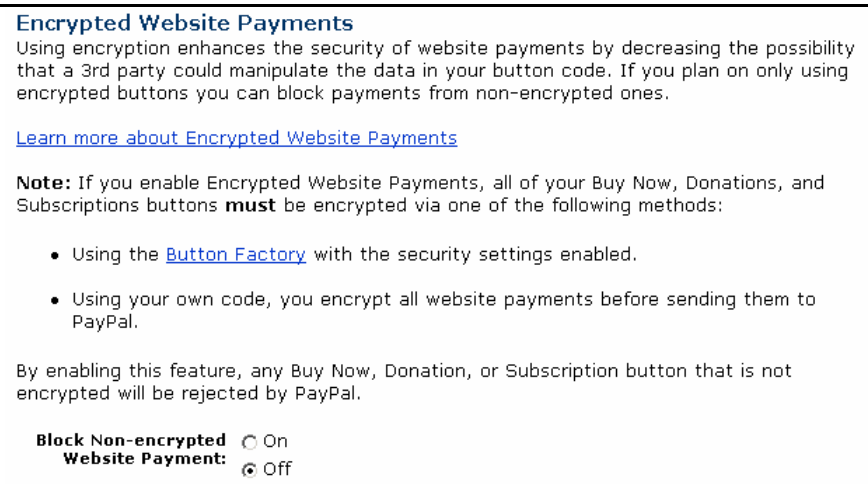
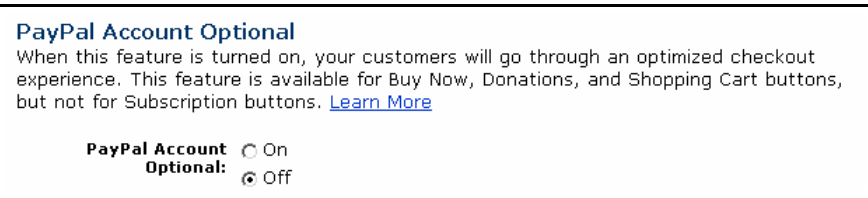
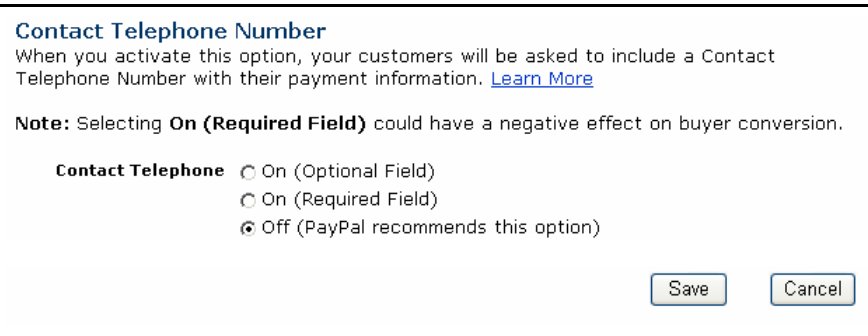


Step 2: Edit necessary settings in "Website Payment Preferences"

Click **Profile** >> Click **Website Payment Preferences** in the **Selling Preferences** section



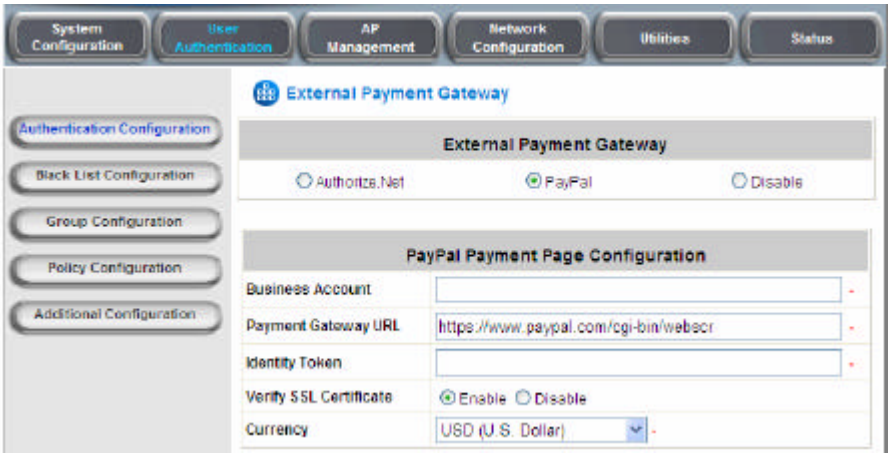
Administrators should scroll down to edit each setting as shown in the table below. To activate all the changes, please click ***Save*** at the end of the page.

Settings	Screenshots
Auto Return (On) **Return URL (Redirect Webpage)** Type http://www.www.com or other URL.	
Payment Data Transfer (On)	
Block Non-encrypted Website Payment (Off)	
PayPal Account Optional (Off)	
Contact Telephone Number (Off) **Click *Save.***	

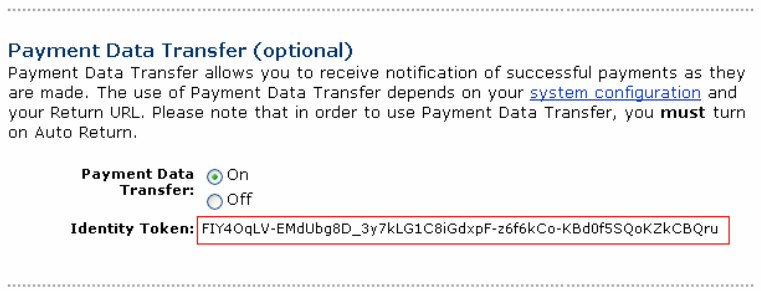
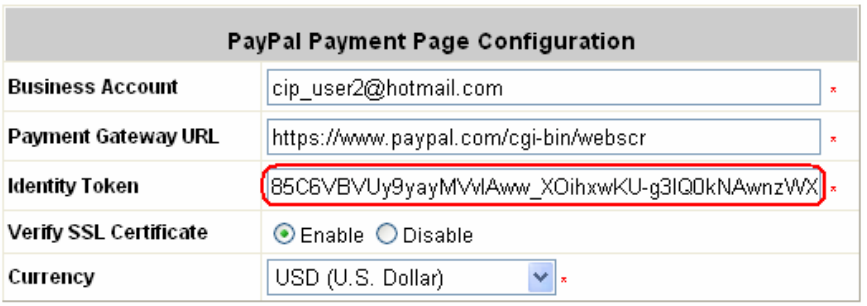
1.2 Configure PheeNet WMS-208 with a PayPal Business Account

Please log in PheeNet WMS-208:

User Authentication >> **Authentication Configuration** >> Click the server ***On-demand User*** >> **External Payment Gateway** >> Click ***Configure*** >> **External Payment Gateway** >> Select ***PayPal***



Three fields are required:

Setting	Description
Business Account ID	This is the "Login ID" (email address) that is associated with the PayPal Business Account.
Payment Gateway URL	https://www.paypal.com/cgi-bin/webscr (default URL for PayPal)
Identity Token	Please log in PayPal after saving the above settings >> Click **Profile** >> Click **Website Payment Preferences** in the **Selling Preferences** section >> Scroll down to the section, **Payment Data Transfer(optional)**.  Copy the **Identity Token** in the above page to the section "**PayPal Payment Page Configuration**" of PheeNet WMS-208. 

1.3 Requirements for Building a Secure PayPal-based E-Commerce Site

To deploy the PayPal function properly, it is required that the merchant register an **Internet domain name** (for example, www.StoreName.com) for this subscriber gateway device.

In addition, it is necessary to sign up for a **SSL certificate**, licensed from a "**Certificate Authority**" (for example, **VerSign**), for this registered Internet domain name.

Thus, by meeting these two requirements, it will allow end customers or subscribers to pay for the Internet access in a securer and convenient way.

2. Basic Maintenance

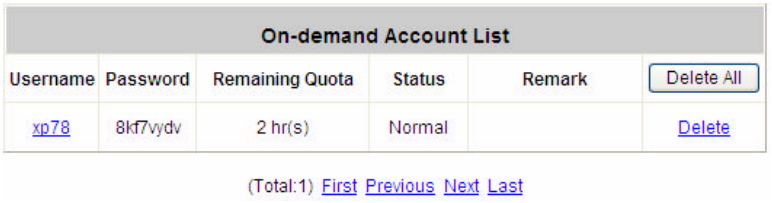
In order to maintain the operation, the merchant owner will have to manage the accounts and payment transactions on PayPal website as well as PheeNet WMS-208.

2.1 Refund a completed payment and remove the on-demand account generated on PheeNet WMS-208

(1) To refund a payment, please log in PayPal >> Click **History** >> Locate the specific payment listing in the activity history log >> Click **Details** of the payment listing >> Click **Refund Payment** at the end of the details page >> Type in information: **Gross Refund Amount** and/or **Optional Note to Buyer** >> Click ***Submit*** >> Confirm the details and click ***Process Refund***

(2) To remove the specific account from PheeNet WMS-208, please log in PheeNet WMS-208:

User Authentication >> **Authentication Configuration** >> Click the server ***On-demand User*** >> **On-demand Account List** >> Click ***View*** >> **On-demand Account List** >> Click ***Delete*** on the record with the account ID. Click ***Delete All*** to delete all users at once.

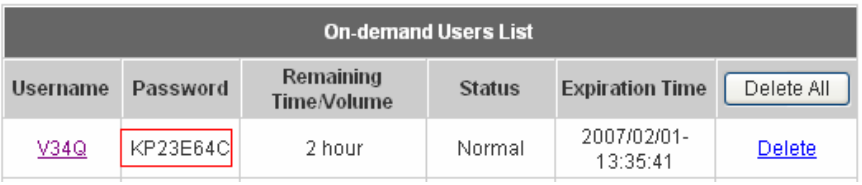


2.2 Find the username and password for a specific customer

(1) To find the username, please log in PayPal >> Click **History** >> Locate the specific payment listing in the activity history log >> Click **Details** of the payment listing >> Username can be found in the ***"Item Title"*** field

(2) To find the password associated with a specific username, please log in PheeNet WMS-208:

User Authentication >> **Authentication Configuration** >> Click the server ***On-demand User*** >> **On-demand Account List** >> Click ***View*** >> **On-demand Account List**. Search for the specific username. Password can be found in the same record



On-demand Users List

Username	Password	Remaining Time/Volume	Status	Expiration Time	Delete All
V34Q	KP23E64C	2 hour	Normal	2007/02/01-13:35:41	Delete

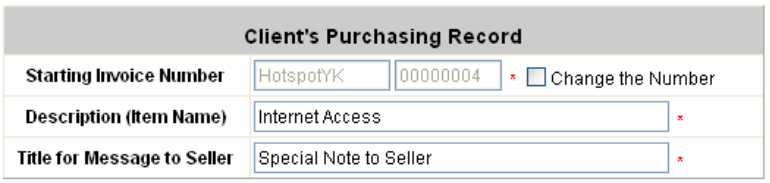
Note:

*As stated by PayPal, you can issue a full or partial refund for any reason and for **60 days** after the original payment was sent. To find the on-demand account name for a specific payment, click **Details** of the payment listing in the activity history log >> **Username** can be found in the **"Item Title"** field*

2.3 Send an email receipt to a customer

If a valid email address is provided, an email receipt with payment details for each successful transaction will be automatically sent to the customer via PayPal. To change the information on the receipt for customer, please log in PheeNet WMS-208:

User Authentication >> **Authentication Configuration** >> Click the server ***On-demand User*** >> **On-demand User Server Configuration** >> **External Payment Gateway** >> Click ***Configure*** >> **External Payment Gateway** >> Select ***PayPal*** >> Go to "**Client's Purchasing Record**" section >> Type in information in the text boxes: **Invoice Number** and **Description (Item Name)** >> Confirm and click ***Apply***



Client's Purchasing Record

Starting Invoice Number	HotspotYK 00000004 *	Change the Number
Description (Item Name)	Internet Access *	
Title for Message to Seller	Special Note to Seller *	

2.4 Send an email receipt for each transaction to the merchant

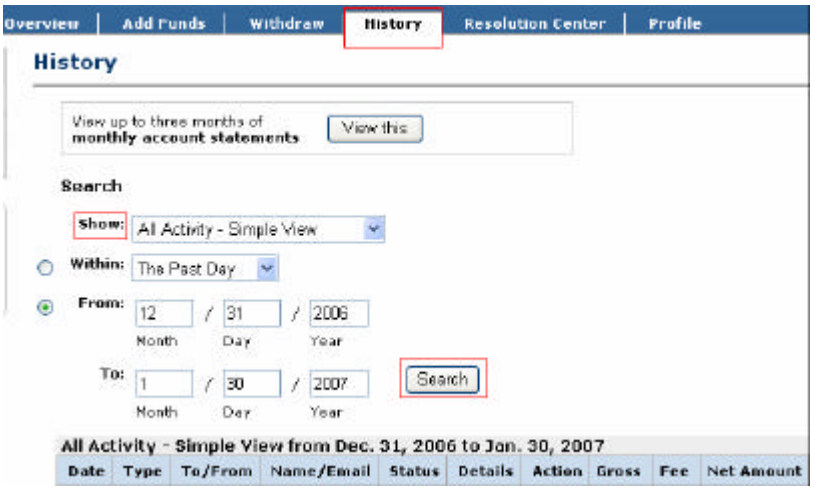
A copy of email receipt with payment details (including available message note from buyer) for each successful transaction will also be automatically sent to the merchant owner/administrator via PayPal.

3. Reporting

During normal operation, the following steps will be necessary to generate transaction reports.

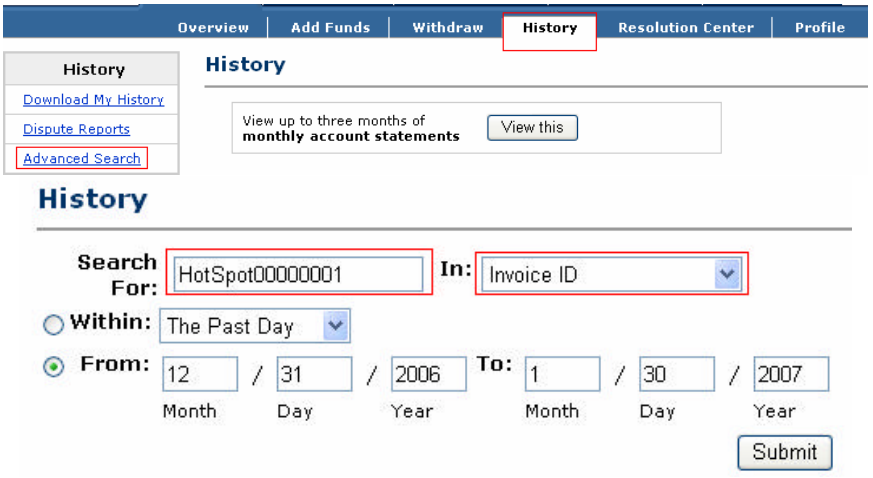
3.1 Transaction activity during a period

(1) Please log in PayPal >> Click **History** >> Choose activity type from the **Show** field as the search criteria >> Specify the dates (**From** and **To** fields) for the period >> Click ***Search***



3.2 Search for the transaction details for a specific customer

Please log in PayPal >> Click **History** >> Click **Advanced Search** >> Enter the name for a specific customer as criteria in the **Search For** field and Choose Last Name or First Name in the **In** field >> Specify the time period >> Click ***Submit*** >> Click **Details** to view the transaction details

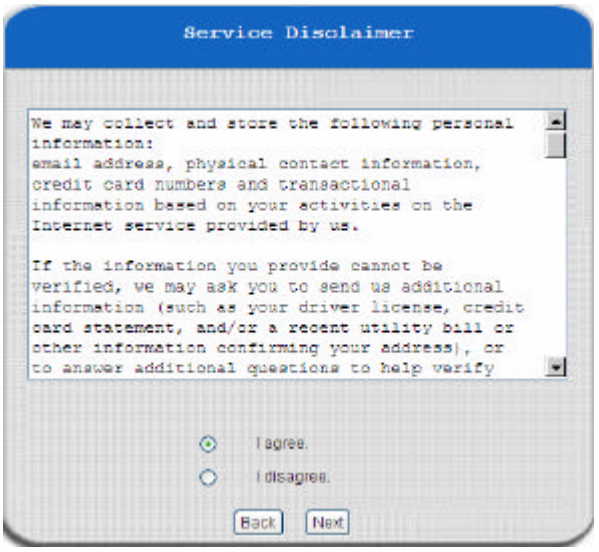


Note: *For more information about PayPal, please see http://www.paypal.com*

4. Examples of Making Payment for End Users

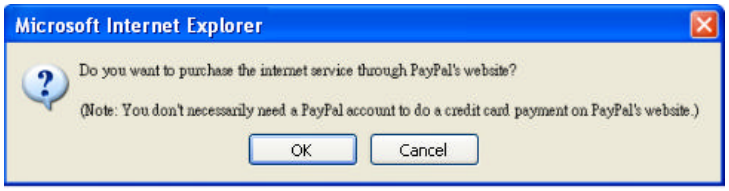
Step 1: Click the link below the login window to pay for the service via PayPal.

Step 2: Choose ***I agree*** to accept the terms of use and click ***Next***.

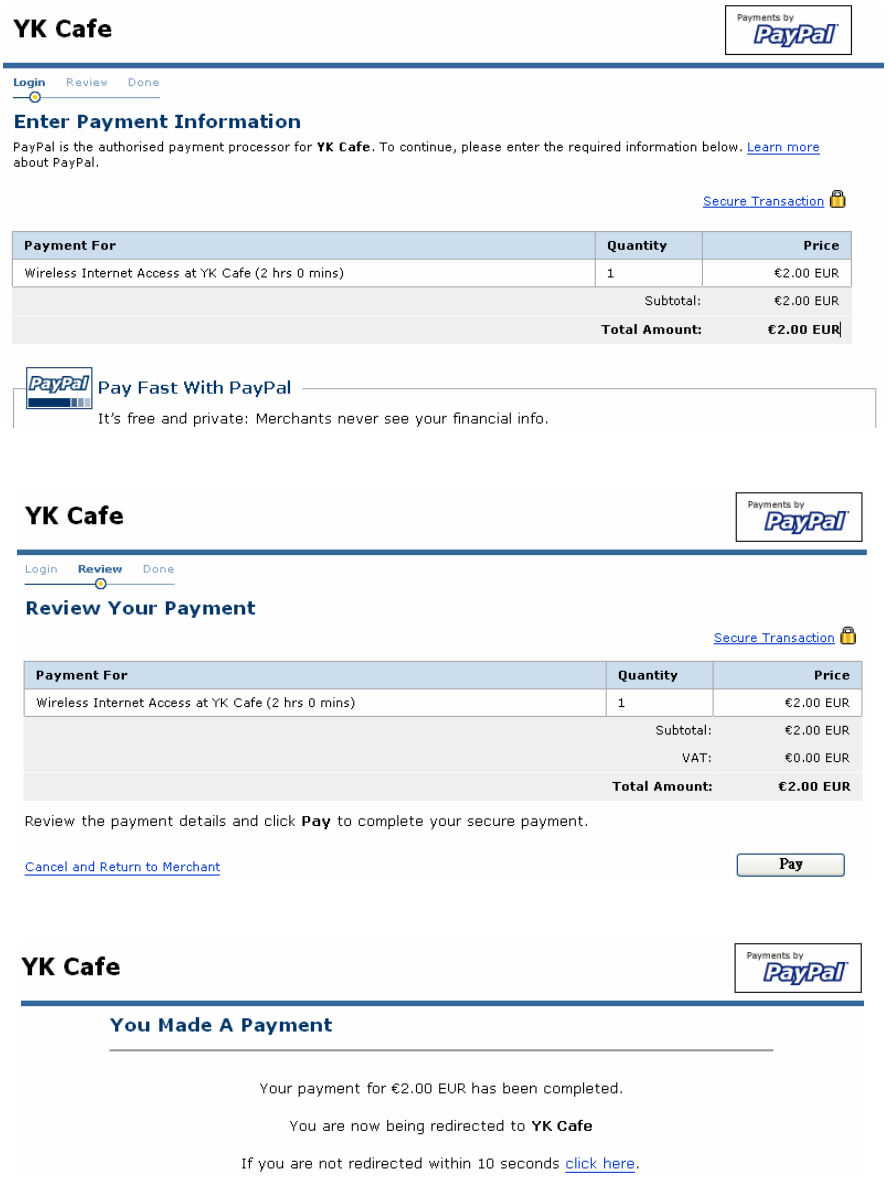

Service Disclaimer
We may collect and store the following personal information:
email address, physical contact information, credit card numbers and transactional information based on your activities on the Internet service provided by us.
If the information you provide cannot be verified, we may ask you to send us additional information (such as your driver license, credit card statement, and/or a recent utility bill or other information confirming your address), or to answer additional questions to help verify
I agree.
I disagree.
Back
Next

Step 3: Please fill out the form and Click ***Submit*** to send out this transaction. There will be a confirm dialog box.

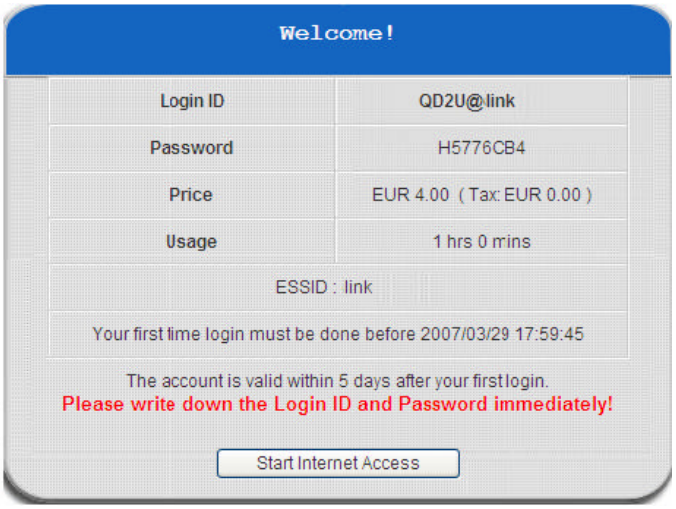
Wireless Internet Access
Rate Plan
Price
1 hrs 0 mins
EUR 4
4 hrs 0 mins
EUR 6
500 Mbyte
EUR 5
Back
Buy Now
Note:
(A)Payment is accepted via PayPal. PayPal enables you to send payments securely online using PayPal account, a credit card or bank account. Clicking on "Buy Now" button, you will be redirected to PayPal's site to make payment. (B) Please don't manually close the browser when you reach PayPal's payment confirmation page. It takes about 30 seconds or more before you are automatically redirected back to our website with a set of Login ID and Password.


Microsoft Internet Explorer
Do you want to purchase the internet service through PayPal's website?
(Note: You don't necessarily need a PayPal account to do a credit card payment on PayPal's website.)
OK
Cancel

Step 4: You will be redirected to PayPal website to complete the payment process.



Step 5: Click ***Start Internet Access*** to use the Internet access service.



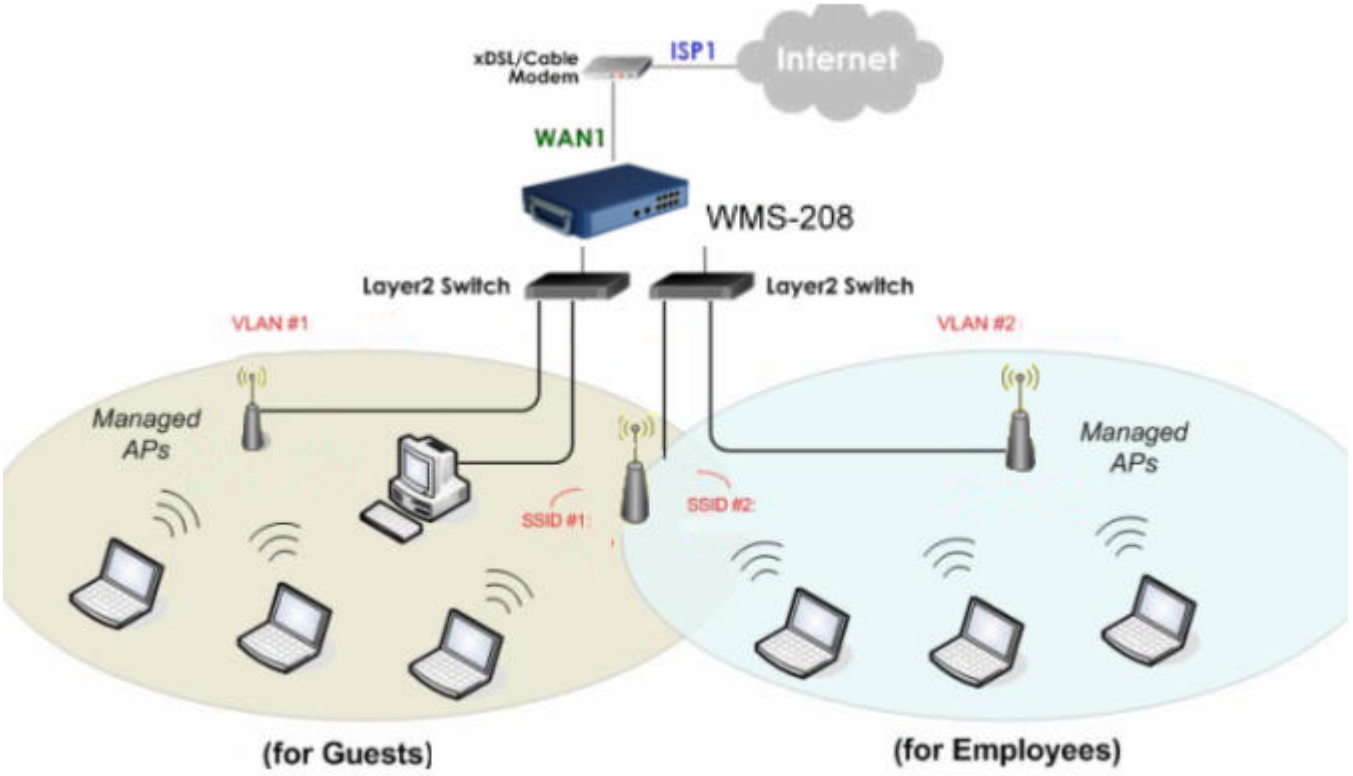
Note:

1) *Payment is accepted via PayPal. PayPal enables you to send payments securely online using PayPal account, a credit card or bank account. Clicking on* ***Buy Now*** *button, you will be redirected to PayPal's site to make payment.*
2) *Please* ***do not manually close the browser*** *when you reach PayPal's payment confirmation page. It takes about 30 seconds or more before you are* ***automatically redirected back to our website with a set of Login ID and Password****.*

Appendix C. Service Zone Deployment Example

▪ Port-Based Service Zone

In **Port-Based** mode, each LAN port can only serve traffic from one Service Zone. An example of network application diagram is shown as below: one Service Zone for **Employees** and another for **Guests**.

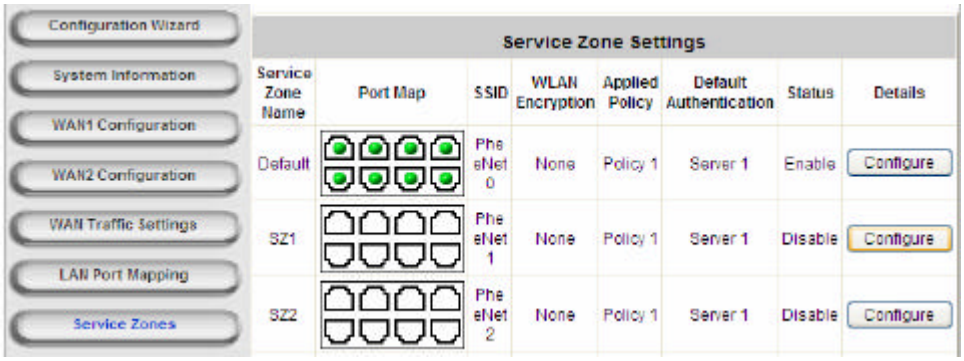


***Note:** The switches deployed under WMS-208 in **Port-Based** mode must be **Layer 2 switches** only.*

• Configuration Steps for Port-Based Service Zones:

Step 1: Configure Service Zone 1 for Guests

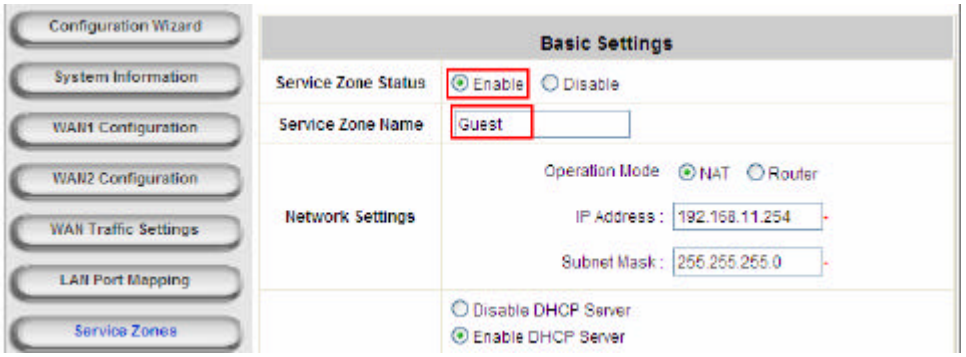
Assume that **LAN1** is assigned to the **Service Zone 1** (**SZ1**) for **Guests**. Click the **System Configuration** menu and select the **Service Zones** tab. Click ***Configure*** of SZ1.



Step 2: Configure Basic Settings for SZ1

Check the ***Enable*** radio button of *Service Zone Status* to activate SZ1.

Enter a name for SZ1 (e.g. **"Guest"**) in the *Service Zone Name* field.

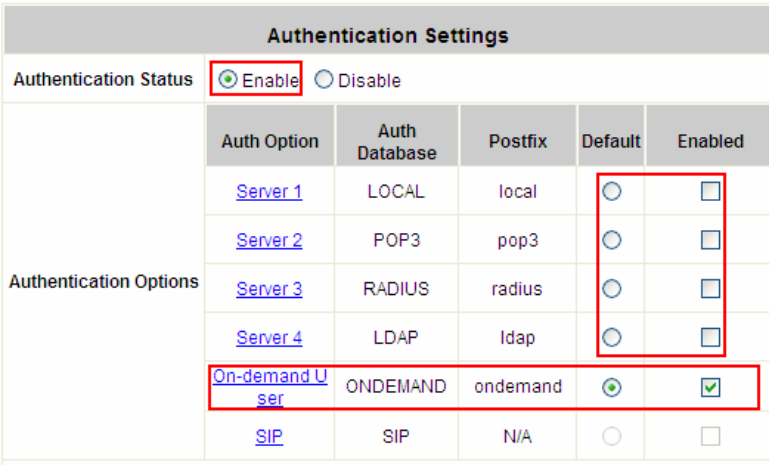


Step 3: Configure Authentication Settings for SZ1

Check the ***Enable*** radio button to enable *Authentication Required for the Zone*.

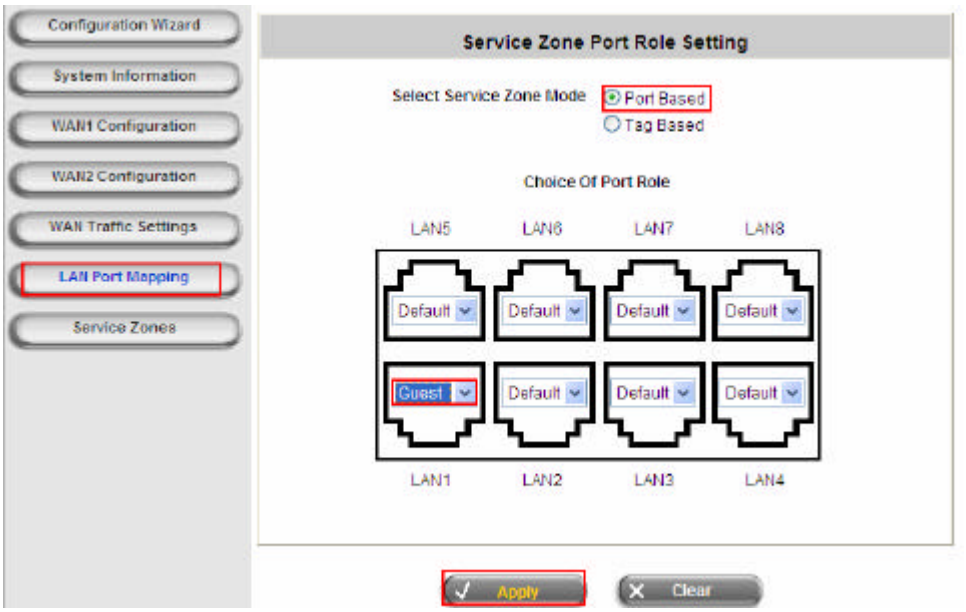
Check the ***Default*** button and ***Enabled*** box of *Guest Users* to set **ONDEMAND** authentication method as default.

Disable all other authentication options. Then, click ***Apply*** to activate the settings made so far. A waming message **"You should restart the system to activate the changes."** will appear at the bottom of the page. Do NOT restart the system until you have completed all the configuration steps.

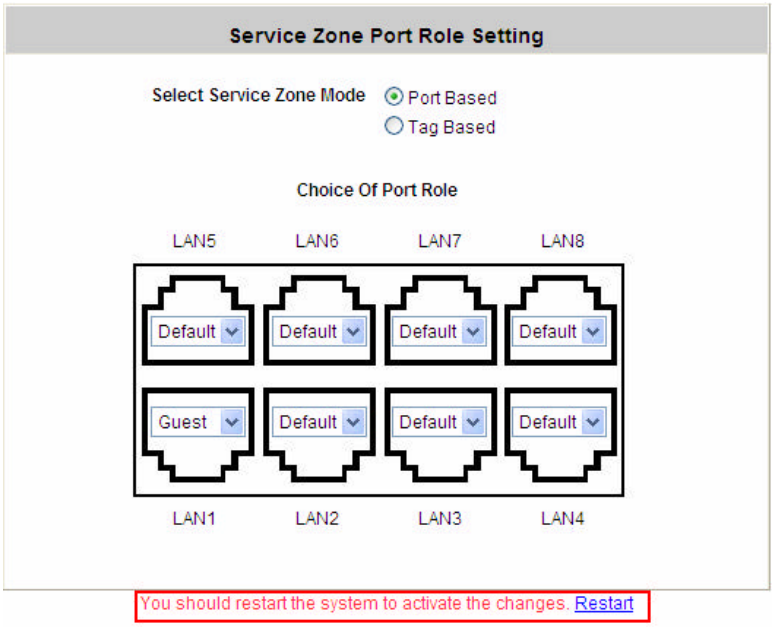


Step 4: Configure LAN Port Mapping for SZ1

Select the **LAN Port Mapping** tab from the ***System*** menu to enter the **LAN Ports and Service Zone Mapping** page. Select *Guests* from the drop-down list box of LAN1. Click ***Apply*** to save the selection.



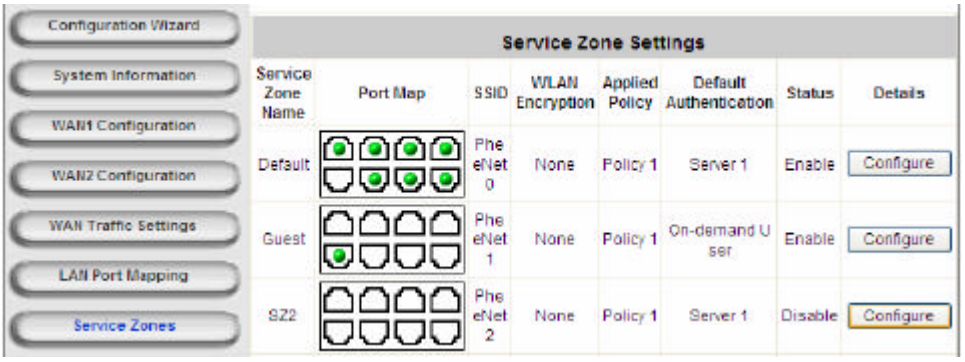
A warning message **"You should restart the system to activate the changes."** will appear at the bottom of the page. Do NOT restart the system until you have completed all the configuration steps.


Service Zone Port Role Setting
Select Service Zone Mode
Port Based
Tag Based
Choice Of Port Role
LAN5 LAN6 LAN7 LAN8
Default Default Default Default
Guest Default Default Default
LAN1 LAN2 LAN3 LAN4
You should restart the system to activate the changes. Restart

LAN1 is now configured for **Guests**.

Step 5: Configure Service Zone 2 for Employees

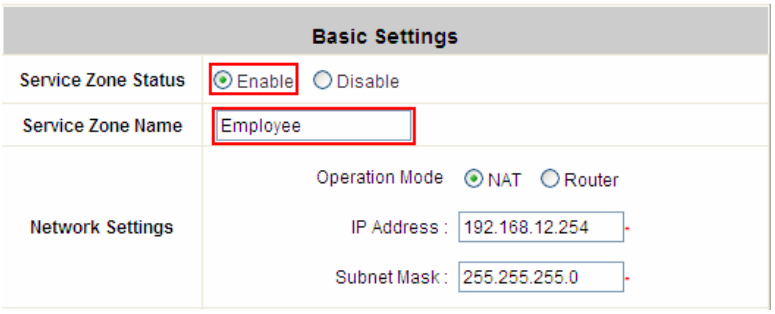
Assume that **LAN2** is assigned to the **Service Zone 2** (**SZ2**) for **Employees**. Select the **Service Zones** tab and click ***Configure*** of SZ2.



Step 6: Configure Basic Settings for SZ2

Check the ***Enable*** radio button of *Service Zone Status* to activate SZ2.

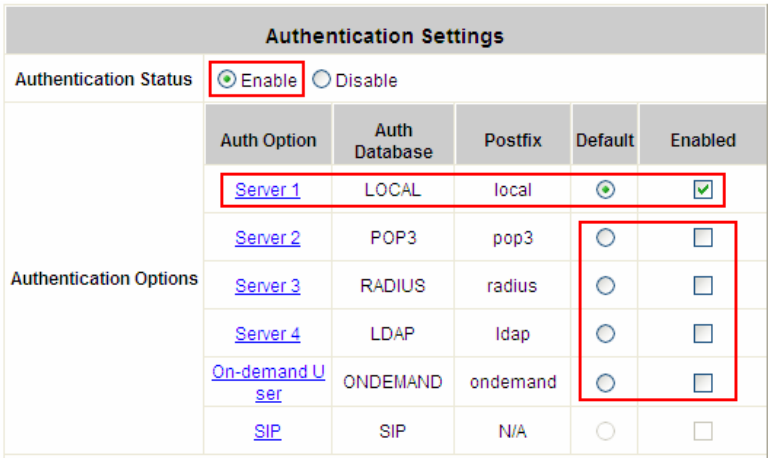
Enter a name for SZ2 (e.g. **"Employee"**) in the *Service Zone Name* field.



Step 7: Configure Authentication Settings for SZ2

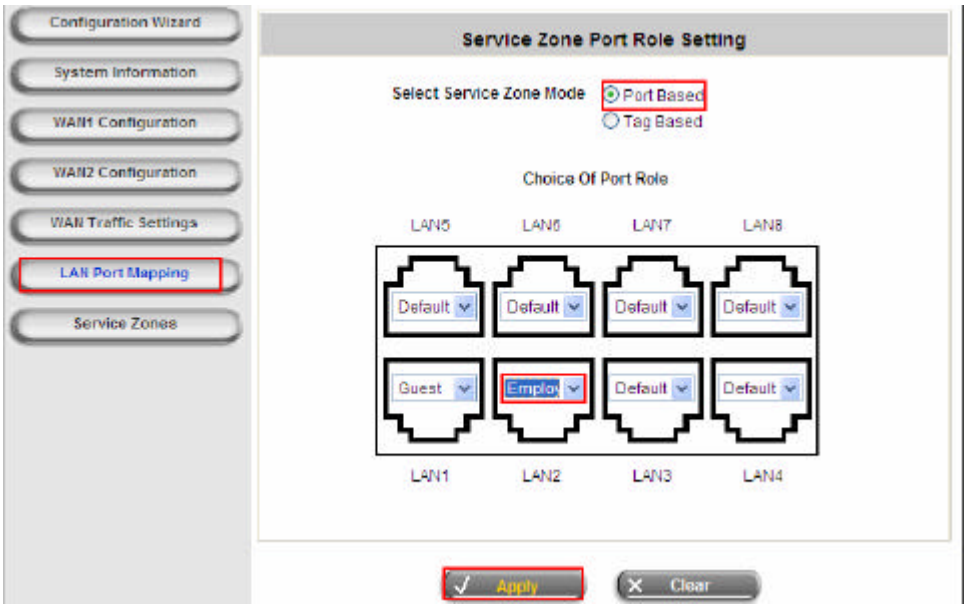
Check the ***Enable*** radio button to enable *Authentication Required for the Zone*.

Check the ***Default*** button and ***Enabled*** box of *Server 1* to set **LOCAL** authentication method as default. Disable all other authentication options. Then, click ***Apply*** to activate the settings made so far. A warning message **"You should restart the system to activate the changes."** will appear at the bottom of the page. Do NOT restart the system until you have completed all the configuration steps.

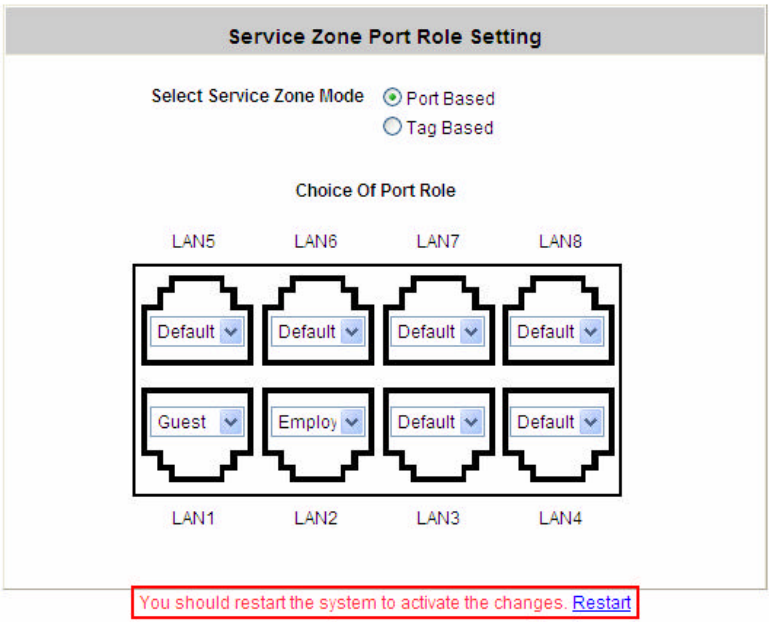


Step 8: Configure LAN Port Mapping for SZ2

Select the **LAN Port Mapping** tab from the ***System*** menu to enter the **LAN Ports and Service Zone Mapping** page. Select *Employee* from the drop-down list box of LAN2. Click ***Apply*** to save the selection.



A warning message **"You should restart the system to activate the changes."** will appear at the bottom of the page. Click the hyperlink of **Restart** to restart the system and activate all configurations.

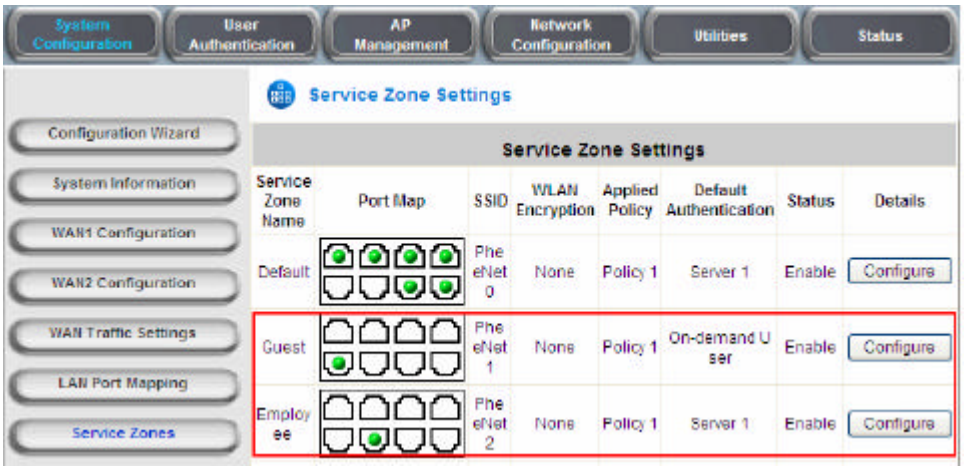

Service Zone Port Role Setting
Select Service Zone Mode
Port Based
Tag Based
Choice Of Port Role
LAN5 LAN6 LAN7 LAN8
Default Default Default Default
Guest Employ Default Default
LAN1 LAN2 LAN3 LAN4
You should restart the system to activate the changes. Restart

Step 9: Restart the System

A confirmation message of **"Do you want to restart the system?"** will appear. Click ***Yes*** to start the restarting process. A confirmation dialog box will then pop out. Click ***OK*** to continue.

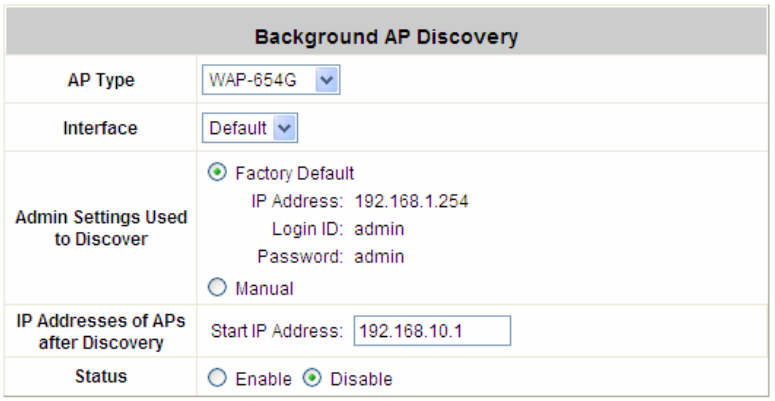
Note: *Please do not interrupt the system during the restarting process.*

Once the settings of two Service Zones are completed, the configured result will be displayed in the **Service Zone Settings** page: **SZ1** and **SZ2** are both enabled.

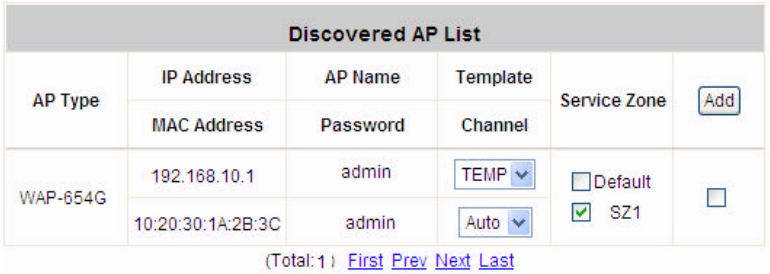


Step 10: AP Discovery

Select **AP Discovery** in **AP Management**. Set the Interface in Default port. Select **Factory Default** in the section of **Admin Settings Used to Discover**. If selecting manually, type the range of IP address in the section. Then start scanning the new APs by clicking ***Scan Now*** button.

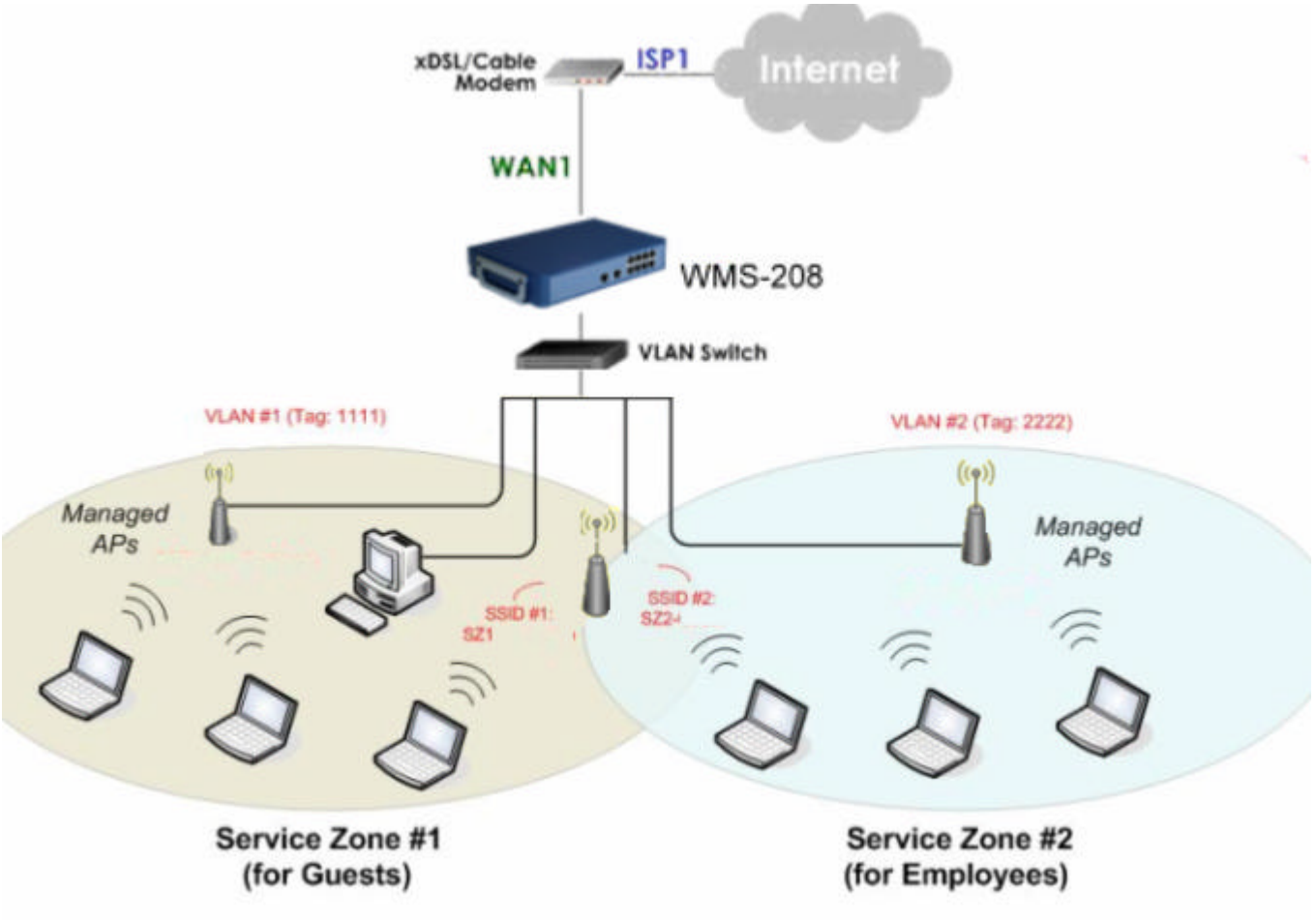


After scanning, new APs will be listed in the **Discovered AP List**. Click the desired Service Zones to add the AP to the list with selected Service Zones.



▪ Tag-Based Service Zone

VLAN tags carried within message frames. An example of network application diagram is shown as below: one Service Zone for **Employees** and another for **Guests**.



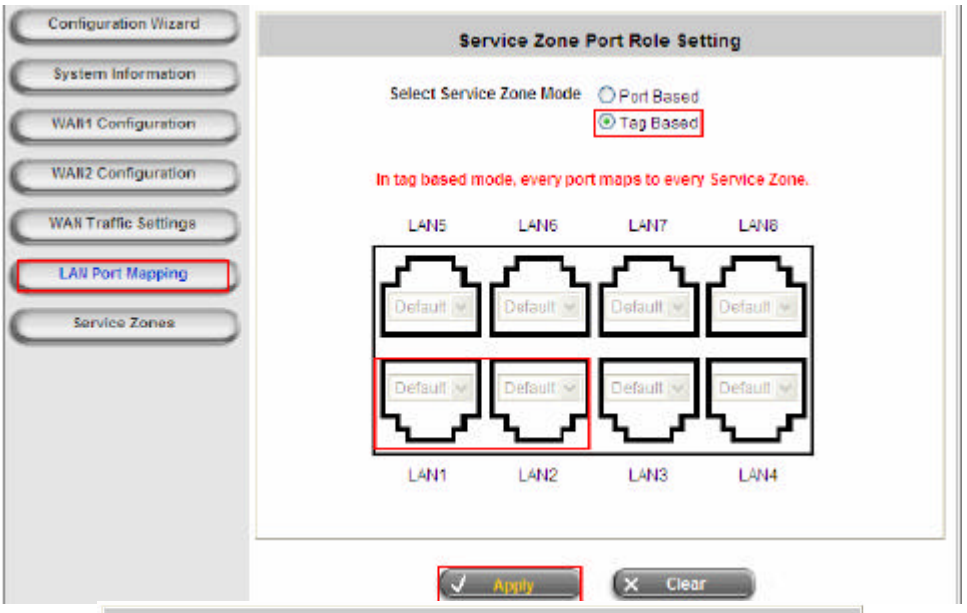
Note: *The switch deployed under WMS-208 in* ***Tag-Based*** *mode must be a* ***VLAN switch*** *only.*

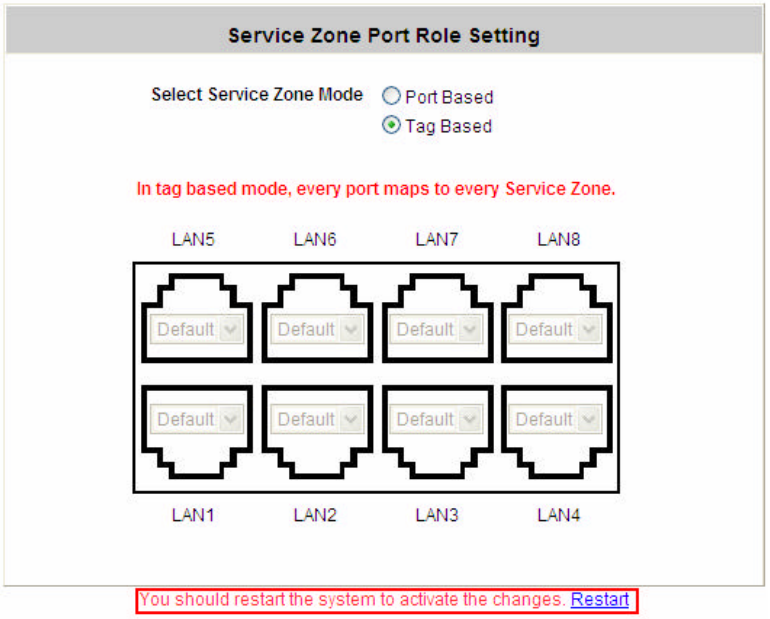
- **Configuration Steps for Tag-Based Service Zones:**

The following example assumes the system is in factory default status and just powered up.

Step 1: Set Tag-Based mode

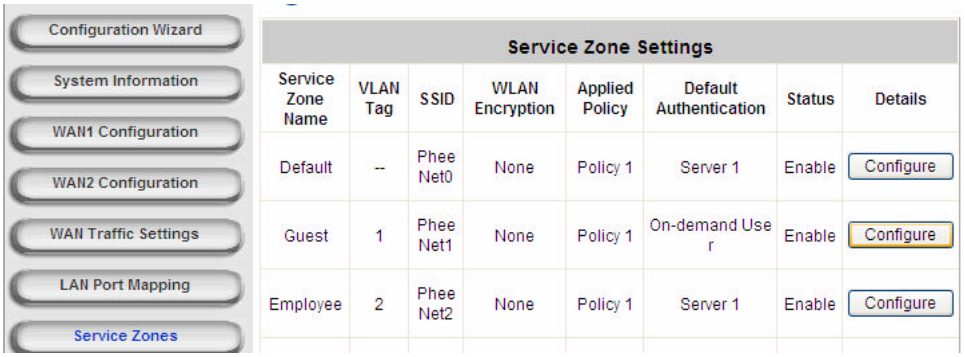
Click the **System** menu and select the **LAN Port Mapping** tab. Select ***Tag-Based*** mode and click ***Apply***. A warning message **"You should restart the system to activate the changes."** will appear at the bottom of the page. Do NOT restart the system until you have completed all the configuration steps.





Step 2: Configure Service Zone 1 for Guest

Select the **Service Zones** tab and click ***Configure*** of SZ1.

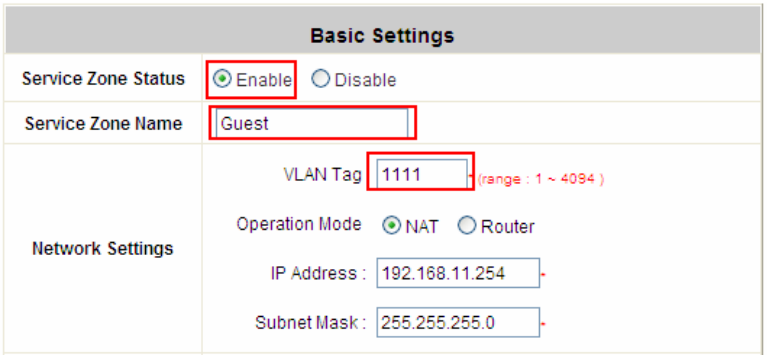


Step 3: Configure Basic Settings for SZ1

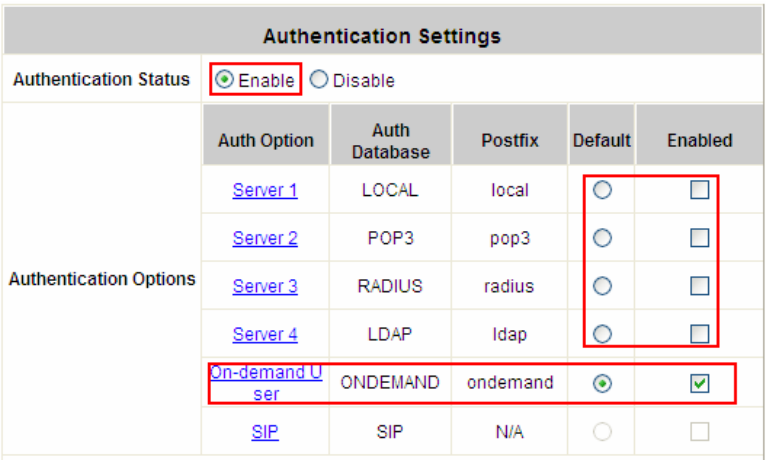
Check the ***Enable*** radio button of *Service Zone Status* to activate SZ1.

Enter a name for SZ1 (e.g. **"Guest"**) in the *Service Zone Name* field.

Enter a VLAN tag for SZ1 (e.g. **"1111"**) in the *VLAN Tag* field.



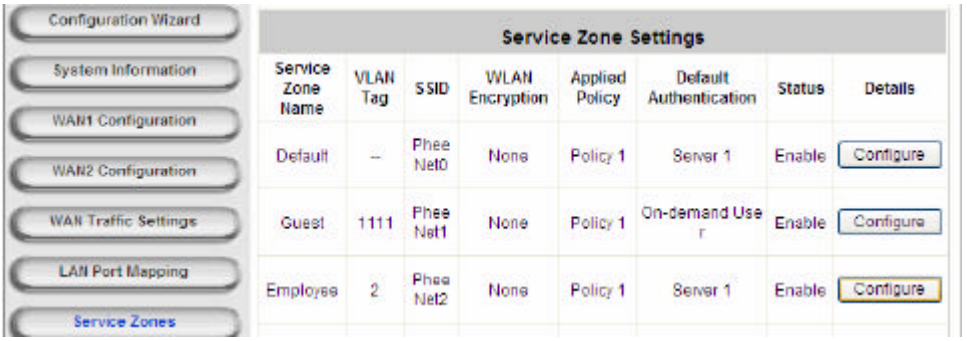
In the **Authentication Settings** section, check the ***Default*** button and ***Enable*** box of *Guest Users* to set **ONDEMAND** authentication method as default. Disable all other authentication options.



Click ***Apply*** to activate the settings. A warning message **"You should restart the system to activate the changes."** will appear at the bottom of the page. Click the hyperlink of **Restart** to restart the system and activate all changes you have made.

Step 4: Configure Service Zone 2 for Employee

Select the **Service Zones** tab and click ***Configure*** of SZ2.

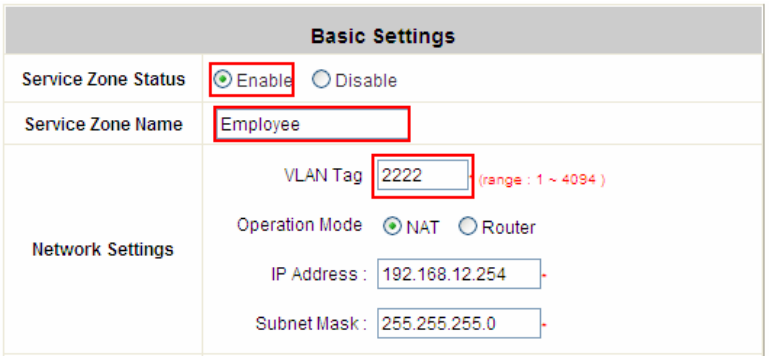


Step 5: Configure Authentication Settings for SZ2

Check the ***Enable*** radio button of *Service Zone Status* to activate SZ2.

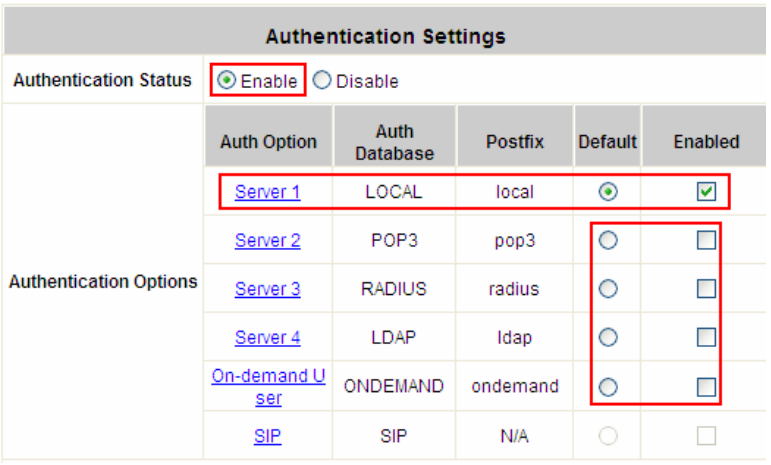
Enter a name for SZ1 (e.g. **"Employee"**) in the *Service Zone Name* field.

Enter a VLAN tag for SZ1 (e.g. **"2222"**) in the *VLAN Tag* field.



Check the ***Enable*** radio button to enable *Authentication Required for the Zone*.

Check the ***Default*** button and ***Enabled*** box of *Server 1* to set **LOCAL** authentication method as default. Disable all other authentication options.



Step 6: Set Policy SZ2

Select **Policy 2** from the drop-down list box.

Click ***Apply*** to activate the settings made so far. A warning message **"You should restart the system to activate the changes."** will appear at the bottom of the page. Do NOT restart the system until you have completed all the configuration steps.

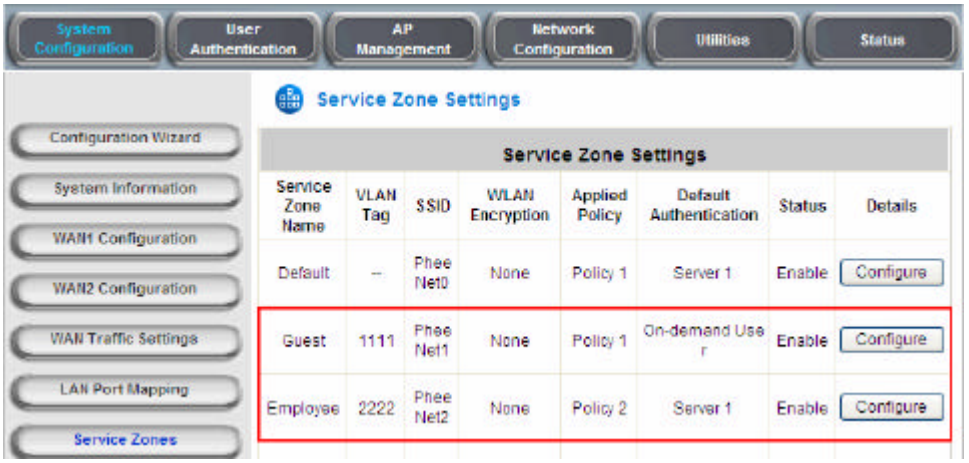
Step 7: Restart the System

Click ***Apply*** to activate the settings. A warning message **"You should restart the system to activate the changes."** will appear at the bottom of the page. Click the hyperlink of **Restart** to restart the system and activate all changes you have made.

A confirmation message of **"Do you want to restart the system?"** will appear. Click ***Yes*** to start the restarting process. A confirmation dialog box will then pop out. Click ***OK*** to continue.

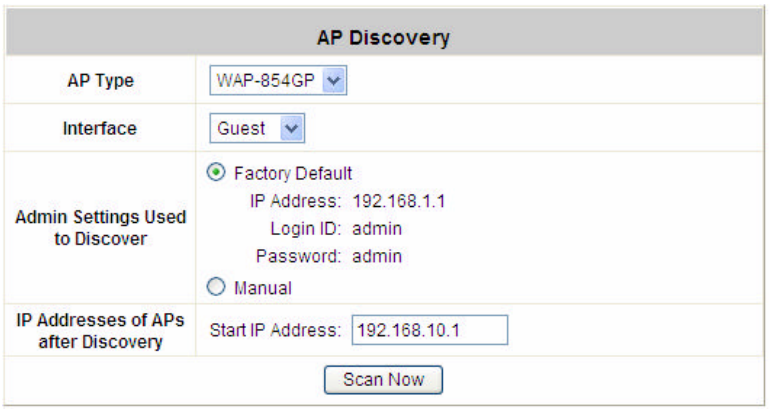
Note: *Please do not interrupt the system during the restarting process.*

Once the settings of two Service Zones are completed, the configured result will be displayed in the **Service Zone Settings** page: **SZ1** and **SZ2** are both enabled.

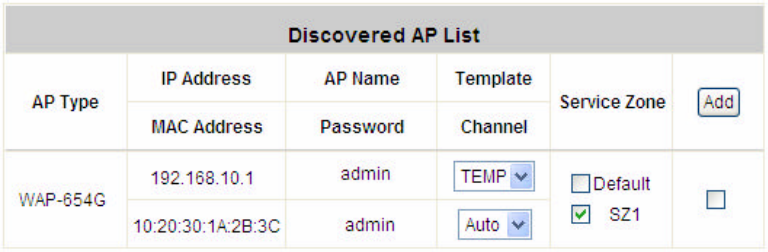


Step 8: AP Discovery

Select **AP Discovery** in **AP Management**. Choose the AP Type, the Interface port has been selected. Select **Factory Default** in the section of **Admin Settings Used to Discover**. If selecting manually, type the range of IP address in the section. Then start scanning the new APs by clicking ***Scan Now*** button.



After scanning, new APs will be listed in the **Discovered AP List**. Click the desired Service Zones for tag-based mode. Add the selected AP with reselected Service Zones to the list by checking the AP and clicking ***Add*** button.

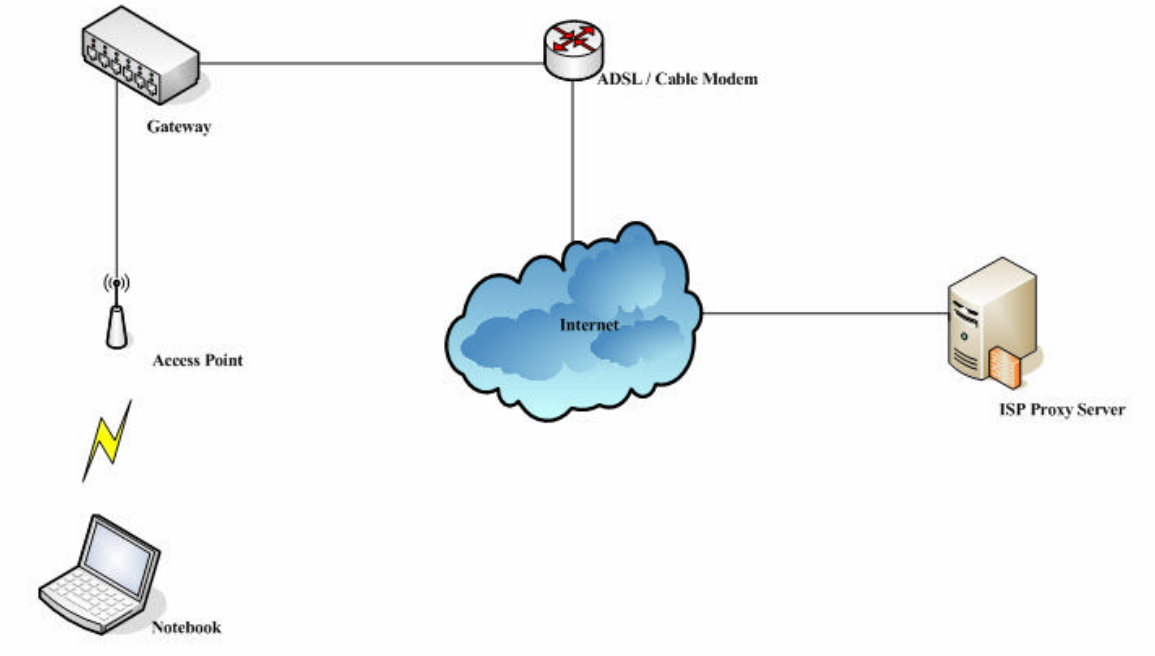


Appendix D. Proxy Setting

Basically, a proxy server can help clients access the network resources more quickly. This section presents basic examples for configuring the proxy server settings of WMS-208.

▪ Using Internet Proxy Server

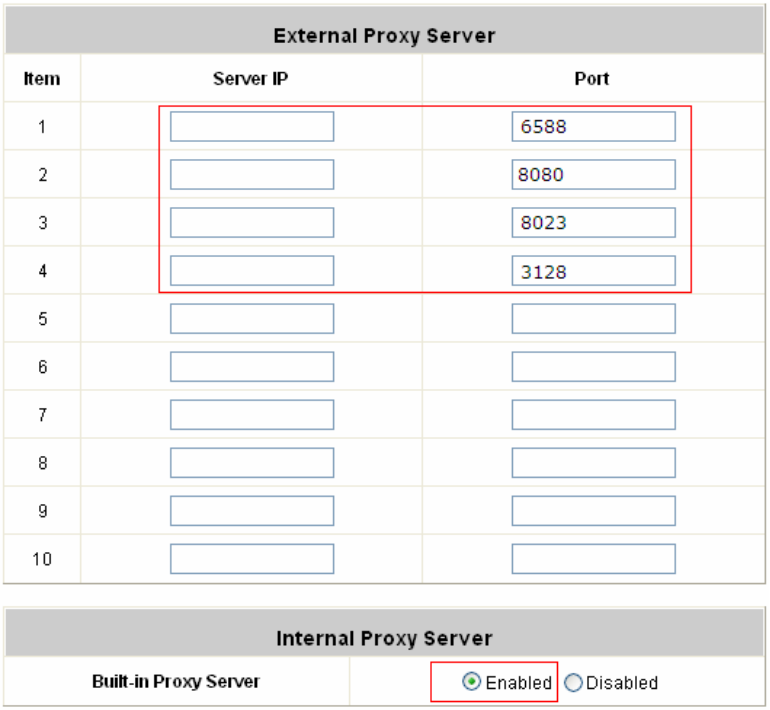
The first scenario is that a proxy server is placed outside the LAN environment or in the Internet. For example, the following diagram shows that a proxy server of an ISP will be used.



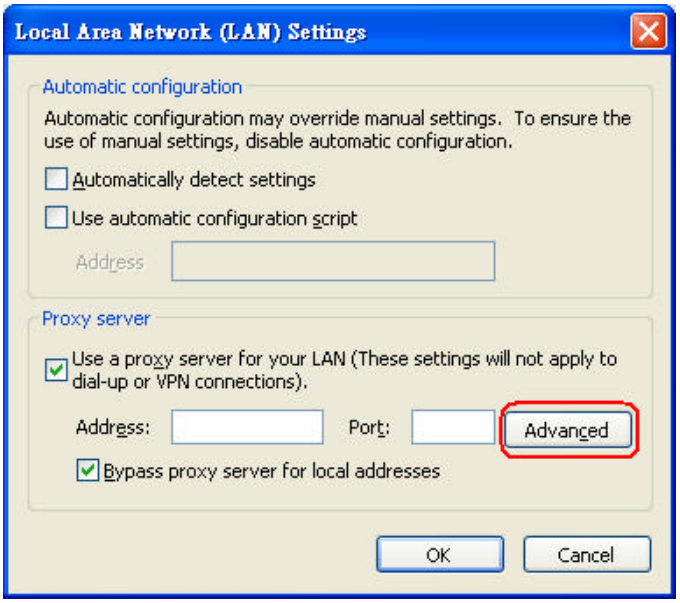
Follow the following steps to complete the proxy configuration:

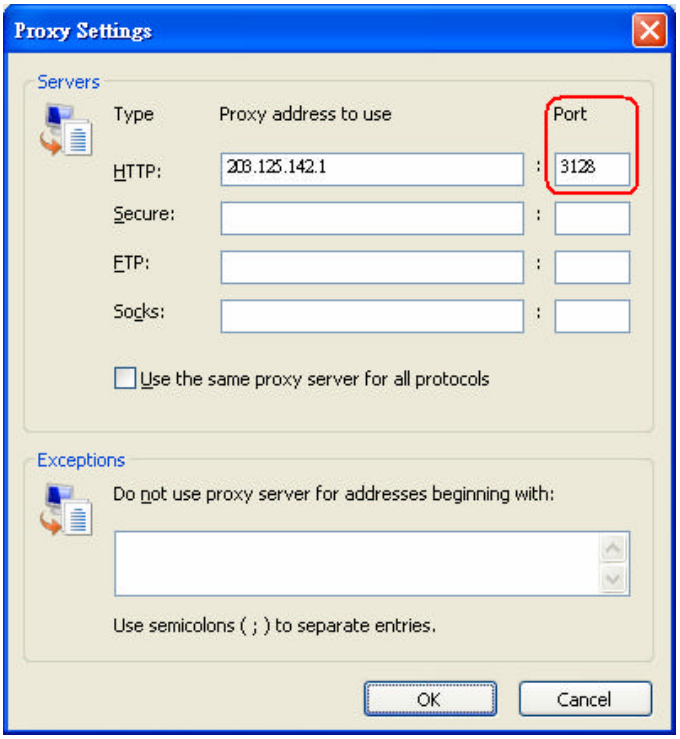
Step 1. Log into the system by using the ***admin*** account.

Step 2. ***Network*** >> ***Proxy Server*** >> ***External Proxy Servers*** page. Add the IP address (leaving it blank means any IP address) and port number of the proxy servers into ***External Proxy Servers*** setting. Enable the ***Built-in Proxy Server***. Click ***Apply*** to save the settings.



Step 3. Make sure that the proxy server settings match with at least one of the proxy server setting of the system – for example, in this case, 203.125.142.1:**3128** matches with blank:**3128**.


Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address:
Port:
Advanced
Bypass proxy server for local addresses
OK
Cancel

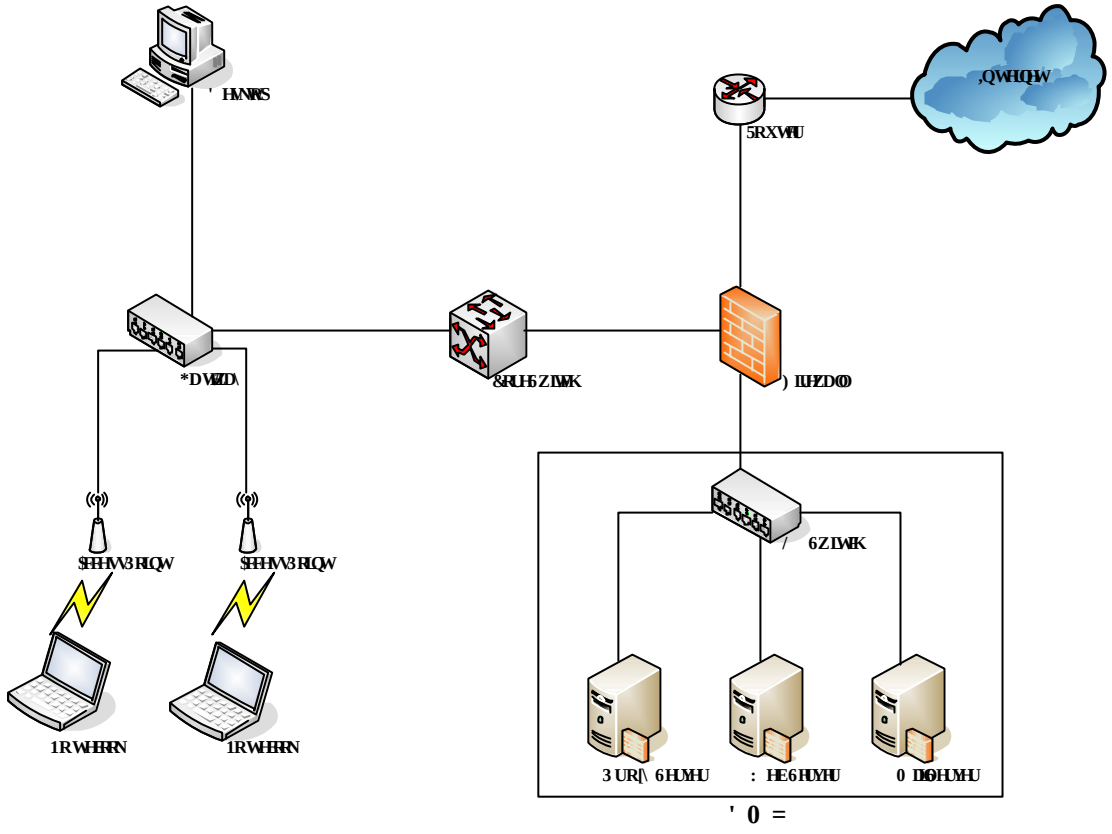


Caution:

1) *It is required that the proxy server setting of the clients match with the proxy server setting of the system. Otherwise, users will not be able to get the Login page for authentication via browsers and it will show an error page in the browser.*
2) *When the **Built-in Proxy Server** is enabled, all the outgoing proxy traffic will be automatically redirected to the built-in proxy server.*

▪ Using Extranet Proxy Server

The second scenario is that a proxy server is placed in the Extranet (such as DMZ), which all users from the Intranet or the Internet are able to access. For example, the following diagram shows that a proxy server of an organization in the DMZ will be used.



Caution:

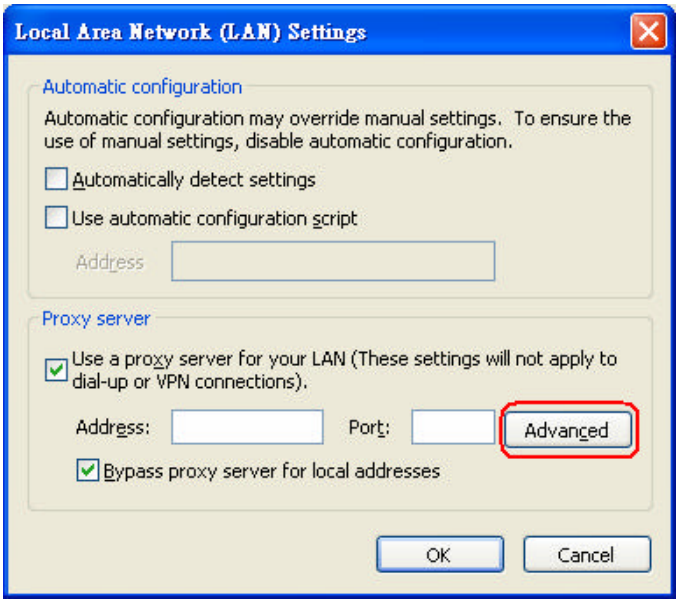
A special scenario is that a proxy server is placed in a zone like Intranet – where users can reach each other without going through the system. In this case, whenever any one of users in the Intranet has been authenticated and connects to the network via the proxy server, other users using the same proxy setting in their browsers will be able to access the network without any authentication. Therefore, to stop the risk, it is strongly recommended to put all proxy servers outside the Intranet.

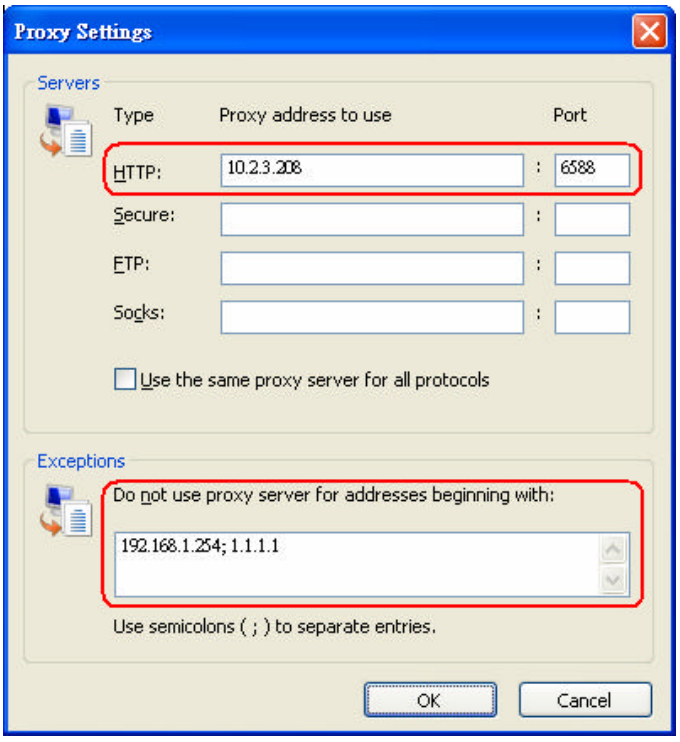
Follow the following steps to complete the proxy configuration:

Step 1. Log in the system by using the ***admin*** account.

Step 2. **Network** >> **Proxy Server** >> **External Proxy Servers** page. Add the IP address and port number of the proxy server into External Proxy Servers setting. Click ***Apply*** to save the settings.

Step 3. Make sure that clients use the same proxy server settings. Please also configure appropriate exceptions if there is any traffic which is not needed to go through proxy server – for example, there is no need to use proxy server for the Default Gateway (192.168.1.254).


Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address:
Port:
Advanced
Bypass proxy server for local addresses
OK
Cancel



Caution:

It is required that the proxy server setting of the clients match with the proxy server setting of the system. Otherwise, users will not be able to get the Login page for authentication via browsers and it will be shown an error page in the browser.

Appendix E. Session Limit and Session Log

▪ Session Limit

To prevent ill-behaved clients or malicious software from using up the system's connection resources, the administrator can restrict the number of concurrent sessions that a user can establish.

- The maximum number of concurrent sessions (TCP and UDP) for each user can be specified in the Global policy, which applies to authenticated users, users on a non-authenticated port, privileged users, and clients in DMZ zones.
- When the number of a user's sessions reaches the session limit (a choice of Unlimited, 10, 25, 50, 100, 200, 350 and 500), the user will be implicitly suspended upon receipt of any new connection request. In this case, a record will be logged to a Syslog server.
- Since this basic protection mechanism may not be able to protect the system from all malicious DoS attacks, it is strongly recommended to build some immune capabilities (such as IDS or IPS solutions) in network deployment to maintain network operation.

▪ Session Log

The system can record connection details of each user accessing the Internet. In addition, the log data can be sent out to a specified Syslog Server, Email Box or FTP Server based on pre-defined interval time.

- The description of the fields of a session log record is shown as below:

Field	Description
Date and Time	The date and time that the session is established
Session Type	[New]: This is a newly established session. [Blocked]: This session is blocked by a Firewall rule.
Username	The account name (with postfix) of the user. When it shows "N.A.", it indicates that the user or device does not need to log in with a username, for example, the user or device is on a non-authenticated port or on the privileged MAC/IP list. Change the account name accordingly, if the name is not identifiable in the record. ***Note:*** *Only 31 characters are allowed for the combination of Session Type plus Username.*
Protocol	The communication protocol of session: TCP or UDP
MAC	The MAC address of the user's computer or device
SIP	The source IP address of the user's computer or device
SPort	The source port number of the user's computer or device
DIP	The destination IP address of the user's computer or device
DPort	The destination port number of the user's computer or device

- An example of session log data is shown as below:

```
31 Aug 12:35:05 2007  [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1626 DIP=203.125.164.132 DPort=80
31 Aug 12:35:05 2007  [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1627 DIP=203.125.164.132 DPort=80
31 Aug 12:35:06 2007  [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1628 DIP=203.125.164.142 DPort=80
31 Aug 12:35:06 2007  [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1629 DIP=203.125.164.142 DPort=80
31 Aug 12:35:07 2007  [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1630 DIP=67.18.163.154 DPort=80
31 Aug 12:35:09 2007  [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1631 DIP=202.43.195.52 DPort=80
31 Aug 12:35:10 2007  [New]user1@local TCP MAC=00:09:6b:cd:83:8c SIP=10.1.1.37 SPort=1632 DIP=203.84.196.242 DPort=80
```

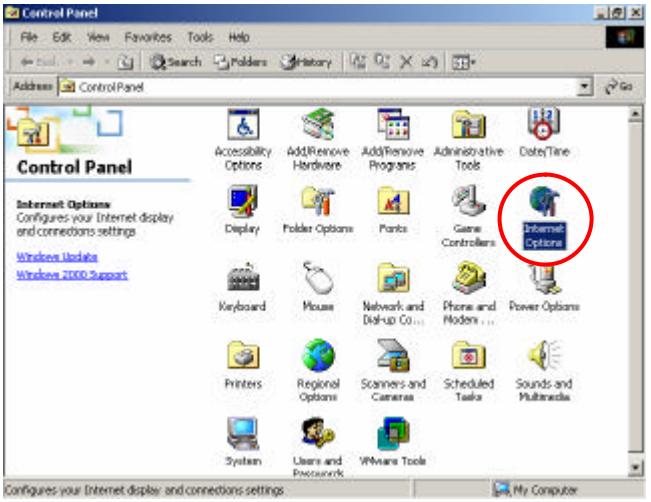
Appendix F. Network Configuration on PC & User Login

▪ Network Configuration on PC

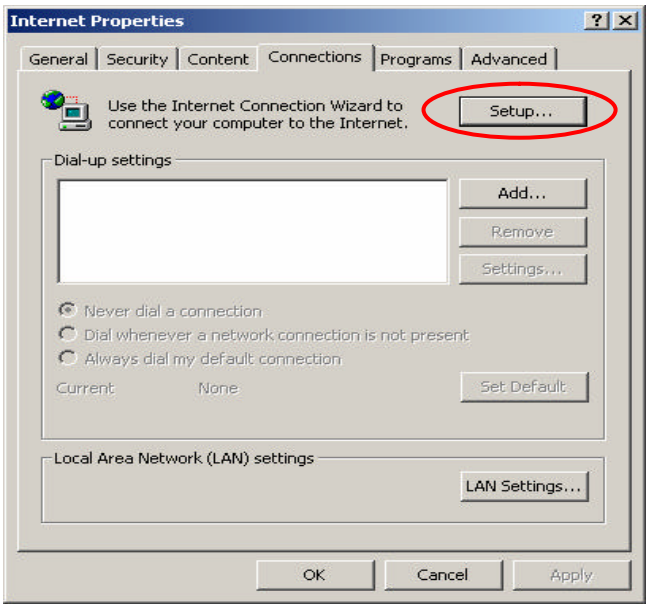
After PheeNet WMS-208 is installed, the following configurations must be set up on the PC: **Internet Connection Setup** and **TCP/IP Network Setup**.

- **Internet Connection Setup**
  - ◆ **Windows 9x/2000**

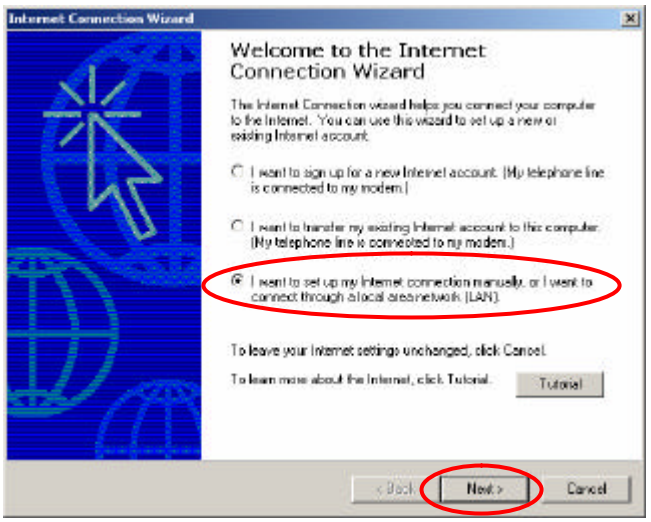
1) Choose **Start** >> **Control Panel** >> **Internet Options**.



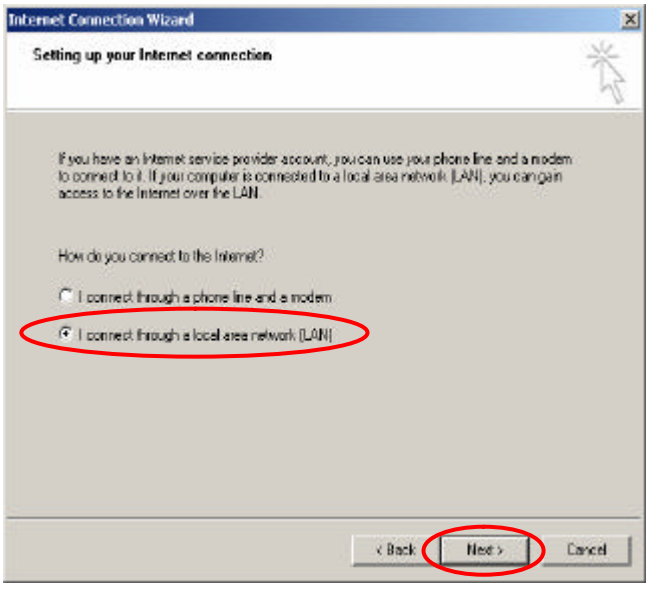
2) Choose the **Connections** tab, and then click ***Setup***.



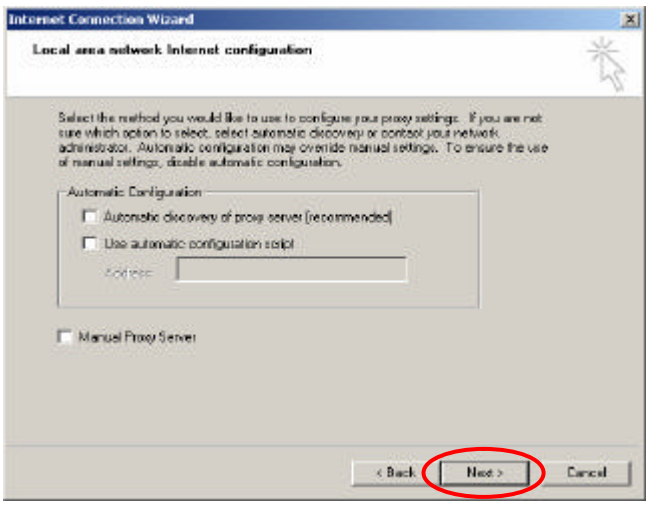
3) Choose **"I want to set up my Internet connection manually, or I want to connect through a local Area network (LAN)"**, and then click ***Next***.


Internet Connection Wizard
Welcome to the Internet Connection Wizard
The Internet Connection wizard helps you connect your computer to the Internet. You can use this wizard to set up a new or existing Internet account.
I want to sign up for a new Internet account. (My telephone line is connected to my modem.)
I want to transfer my existing Internet account to this computer. (My telephone line is connected to my modem.)
I want to set up my Internet connection manually, or I want to connect through a local area network (LAN).
To leave your Internet settings unchanged, click Cancel.
To learn more about the Internet, click Tutorial.
Tutorial
< Back
Next >
Cancel

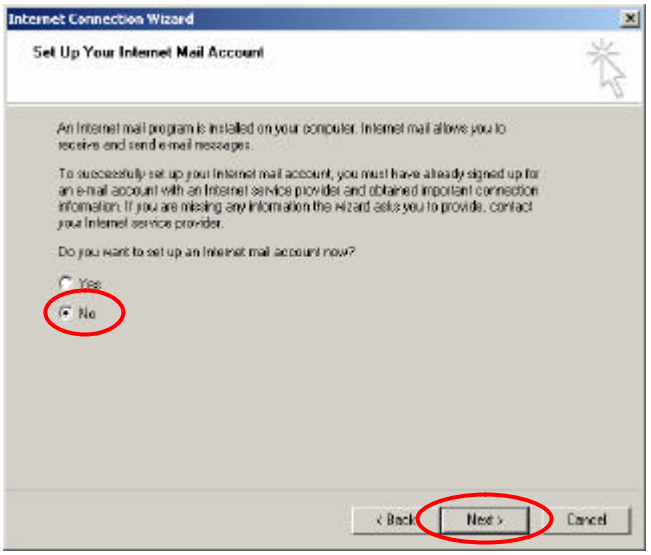
4) Choose **"I connect through a local area network (LAN)"** and then click ***Next***.


Internet Connection Wizard
Setting up your Internet connection
If you have an Internet service provider account, you can use your phone line and a modem to connect to it. If your computer is connected to a local area network (LAN), you can gain access to the Internet over the LAN.
How do you connect to the Internet?
I connect through a phone line and a modem
I connect through a local area network (LAN)
< Back
Next >
Cancel

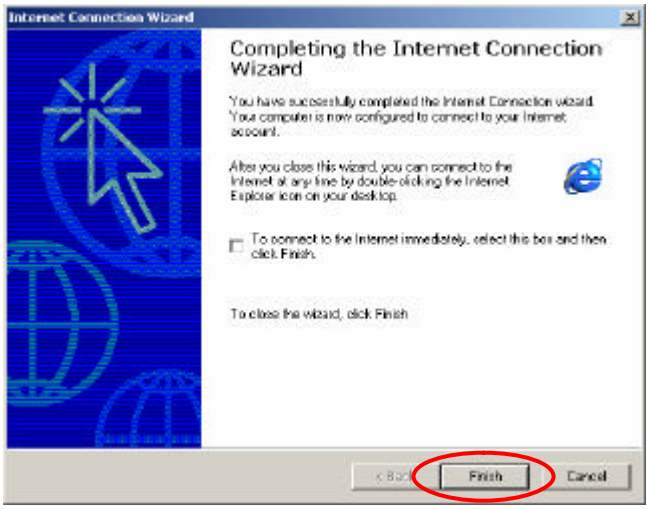
5) **DO NOT** choose any option in the following LAN window for Internet configuration, and just click ***Next***.


Internet Connection Wizard
Local area network Internet configuration
Select the method you would like to use to configure your proxy settings. If you are not sure which option to select, select automatic discovery or contact your network administrator. Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatic Configuration
Automatic discovery of proxy server (recommended)
Use automatic configuration script
Address
Manual Proxy Server
< Back
Next >
Cancel

6) Choose **"No"** and then click ***Next***.

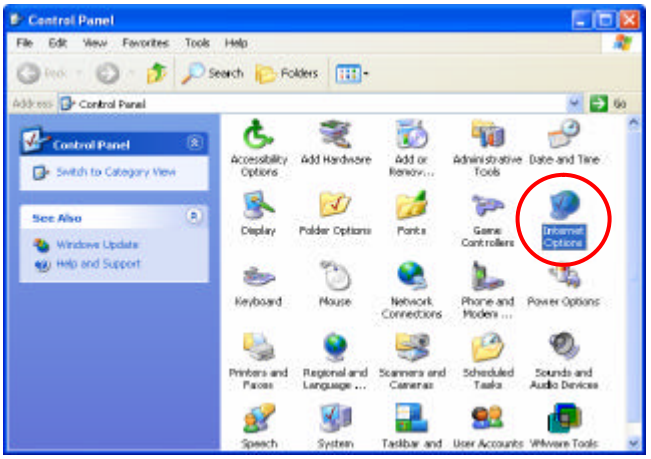

Internet Connection Wizard
Set Up Your Internet Mail Account
An Internet mail program is installed on your computer. Internet mail allows you to receive and send e-mail messages.
To successfully set up your Internet mail account, you must have already signed up for an e-mail account with an Internet service provider and obtained important connection information. If you are missing any information the wizard asks you to provide, contact your Internet service provider.
Do you want to set up an Internet mail account now?
Yes
No
< Back
Next >
Cancel

7) Finally, click ***Finish*** to exit the **Internet Connection Wizard**. Now, the set up is completed.

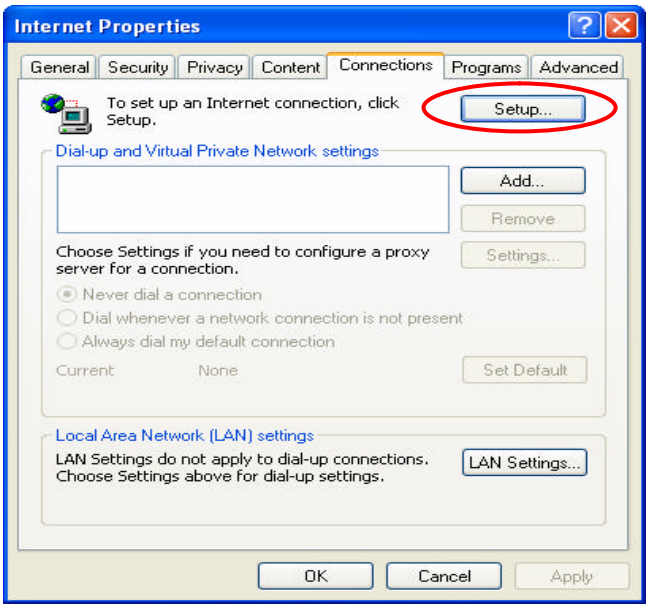

Internet Connection Wizard
Completing the Internet Connection Wizard
You have successfully completed the Internet Connection wizard. Your computer is now configured to connect to your Internet account.
After you close this wizard, you can connect to the Internet at any time by double-clicking the Internet Explorer icon on your desktop.
To connect to the Internet immediately, select this box and then click Finish.
To close the wizard, click Finish
Finish
Cancel

◆ **Windows XP**

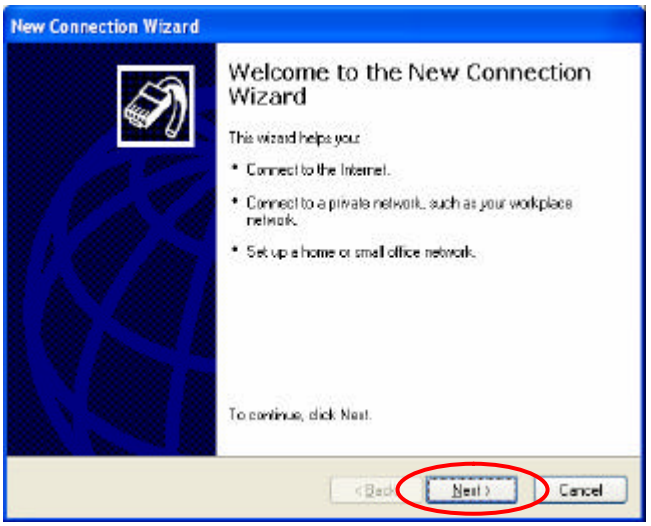
1) Choose **Start** >> **Control Panel** >> **Internet Option**.



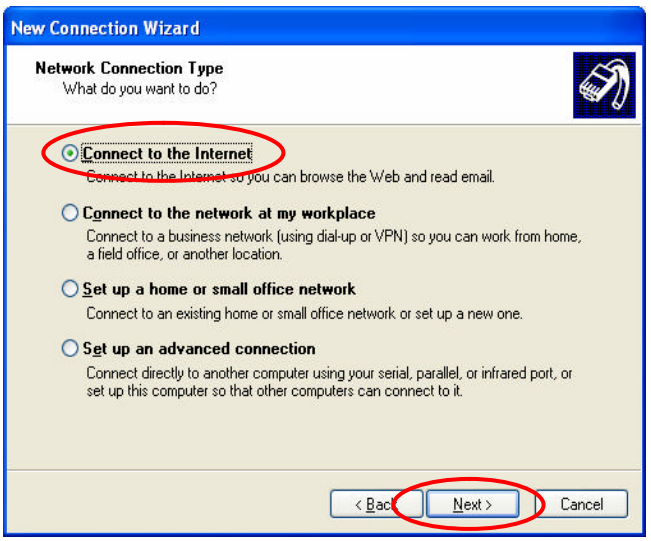
2) Choose the **Connections** tab, and then click ***Setup***.



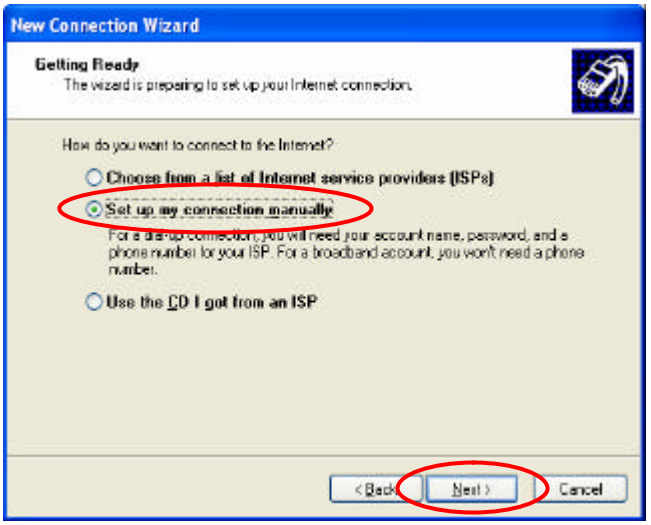
3) When the **Welcome to the New Connection Wizard** window appears, click ***Next***.


New Connection Wizard
Welcome to the New Connection Wizard
This wizard helps you:
Connect to the Internet.
Connect to a private network, such as your workplace network.
Set up a home or small office network.
To continue, click Next.
< Back
Next >
Cancel

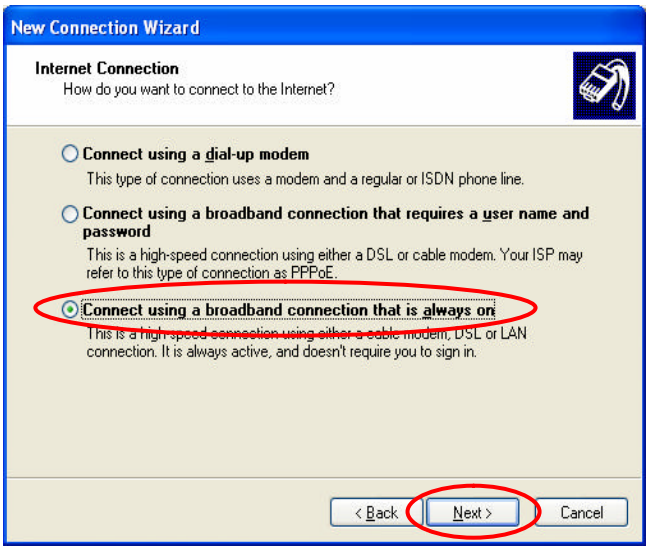
4) Choose **"Connect to the Internet"** and then click ***Next***.


New Connection Wizard
Network Connection Type
What do you want to do?
Connect to the Internet
Connect to the Internet so you can browse the Web and read email.
Connect to the network at my workplace
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.
Set up a home or small office network
Connect to an existing home or small office network or set up a new one.
Set up an advanced connection
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.
< Back
Next >
Cancel

5) Choose **"Set up my connection manually"** and then click ***Next***.


New Connection Wizard
Getting Ready
The wizard is preparing to set up your Internet connection.
How do you want to connect to the Internet?
Choose from a list of Internet service providers (ISPs)
Set up my connection manually
For a dial-up connection, you will need your account name, password, and a phone number for your ISP. For a broadband account, you won't need a phone number.
Use the CD I got from an ISP
< Back
Next >
Cancel

6) Choose **"Connect using a broadband connection that is always on"** and then click ***Next***.


New Connection Wizard
Internet Connection
How do you want to connect to the Internet?
Connect using a dial-up modem
This type of connection uses a modem and a regular or ISDN phone line.
Connect using a broadband connection that requires a user name and password
This is a high-speed connection using either a DSL or cable modem. Your ISP may refer to this type of connection as PPPoE.
Connect using a broadband connection that is always on
This is a high-speed connection using either a cable modem, DSL or LAN connection. It is always active, and doesn't require you to sign in.
< Back
Next >
Cancel

7) Finally, click ***Finish*** to exit the **Connection Wizard**. Now, the setup is completed.

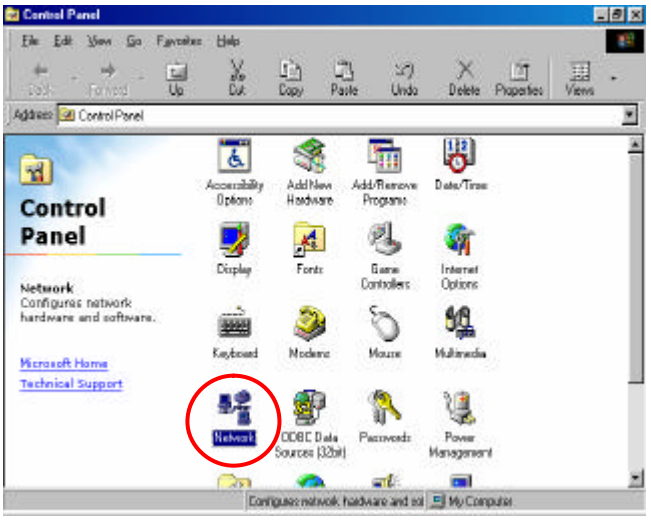
New Connection Wizard
Completing the New Connection Wizard
Your broadband connection should already be configured and ready to use. If your connection is not working properly, click the following link.
Learn more about broadband connections.
To close this wizard, click Finish.
< Back
Finish
Cancel

- **TCP/IP Network Setup**

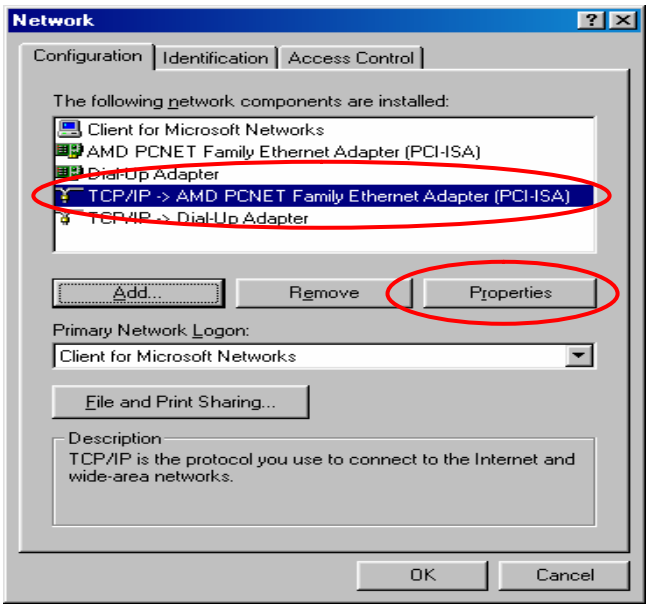
If the operating system of the PC in use is Windows 95/98/ME/2000/XP, keep the default settings without any changes to directly start/restart the system. With the factory default settings, during the process of starting the system, PheeNet WMS-208 with DHCP function will automatically assign an appropriate IP address and related information for each PC. If the Windows operating system is not a server version, the default settings of the TCP/IP will regard the PC as a DHCP client, and this function is called **"Obtain an IP address automatically"**. If checking the TCP/IP setup or using the static IP in the LAN1/LAN2 or LAN3/LAN4 section is desired, please follow these steps:

◆ **Check the TCP/IP Setup of Window 9x/ME**

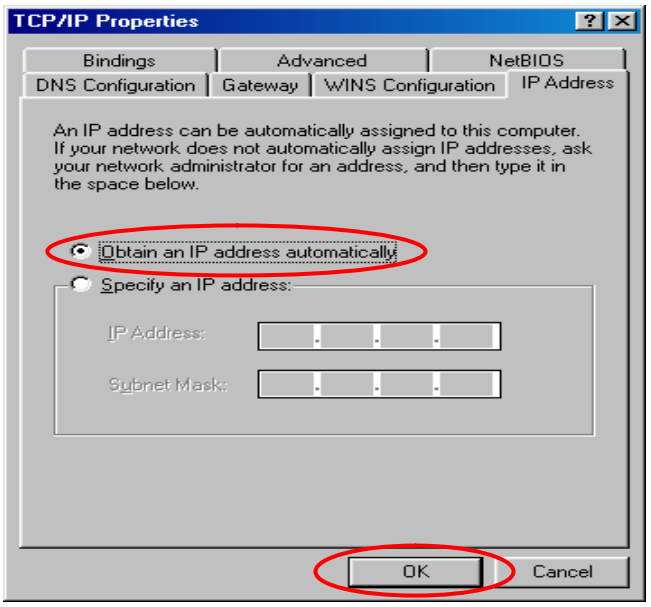
1) Choose **Start** >> **Control Panel** >> **Network**.



2) Click on the **Configuration** tab and select **"TCP/IP** >> **AMD PCNET Family Ethernet Adapter (PCI-ISA)"**, and then click ***Properties***. Now, you can choose to use DHCP or a specific IP address.



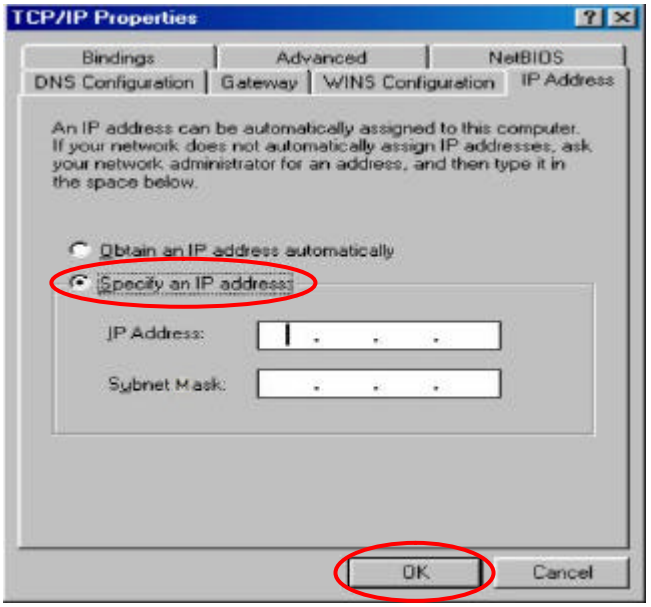
3) **Using DHCP:** If you want to use DHCP, click on the **IP Address** tab and choose **"Obtain an IP address automatically"**, and then click ***OK***. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from WMS-208.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

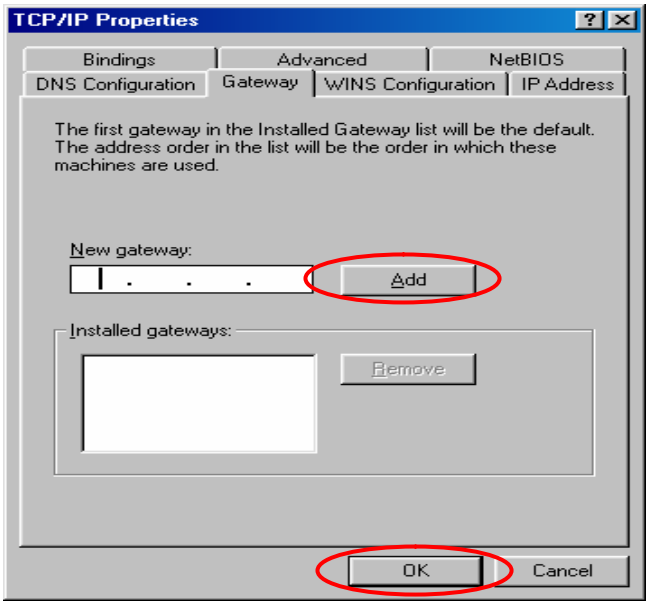
4) **Using Specific IP Address:** If you want to use a specific IP address, acquire the following information from the network administrator: the *IP Address*, *Subnet Mask* and *DNS Server address* provided by your ISP and the *Gateway address* of WMS-208.

Note: *If your PC has been set up completed, please inform the network administrator before proceeding to the following steps.*

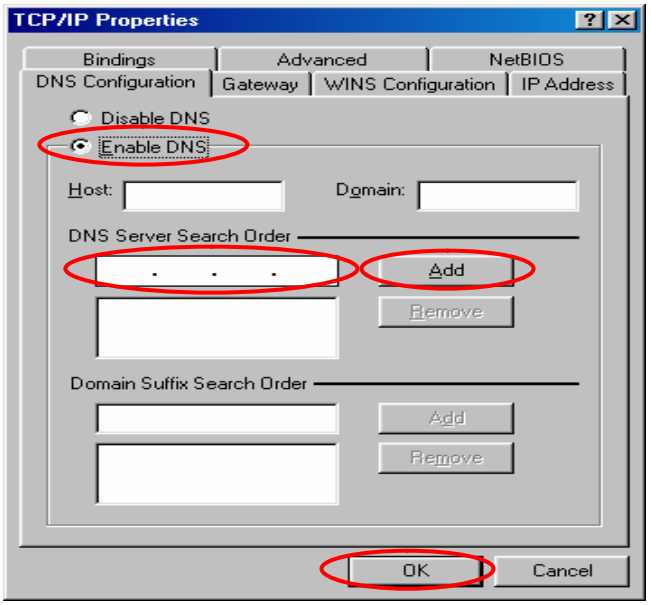
4.1) Click on the **IP Address** tab and choose **"Specify an IP address"**. Enter the *IP Address*, *Subnet Mask* and then click ***OK***.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

4.2) Click on the **Gateway** tab. Enter the gateway address of WMS-208 in the **"New gateway"** field and click ***Add***. Then, click ***OK***.



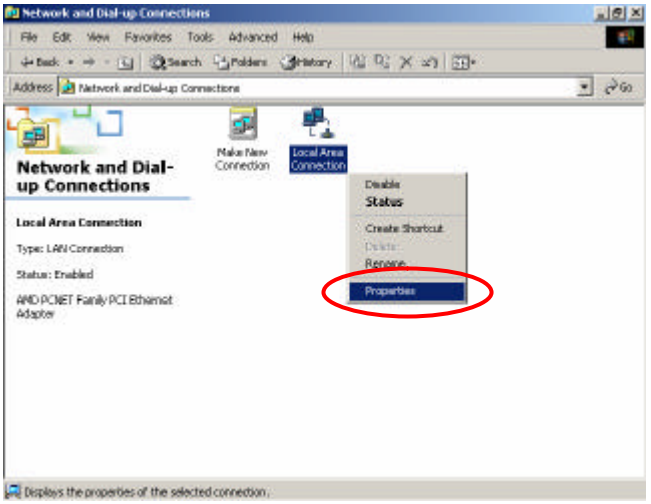
4.3) Click on **DNS Configuration** tab. If the DNS Server field is empty, select **"Enable DNS"** and enter *DNS Server address*. Click ***Add***, and then click ***OK*** to complete the configuration.



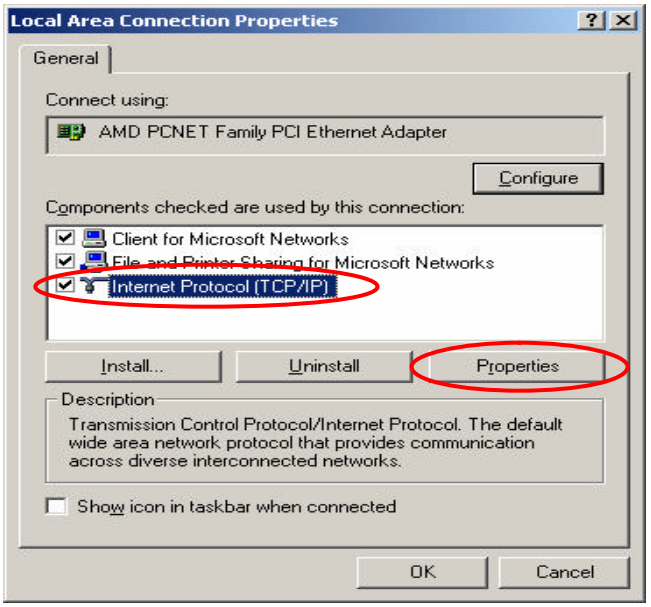
◆ **Check the TCP/IP Setup of Window 2000**

1) Select **Start** >> **Control Panel** >> **Network and Dial-up Connections**.

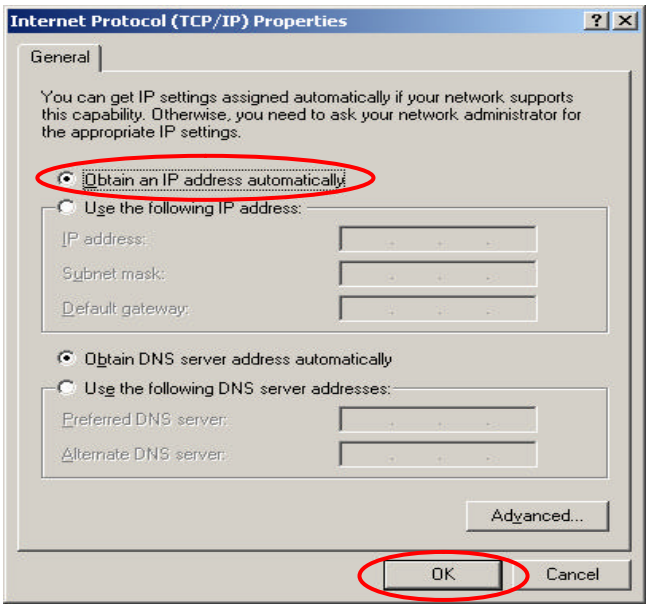
2) Right click on the **Local Area Connection** icon and select **"Properties"**.



3) Select **"Internet Protocol (TCP/IP)"** and then click ***Properties***. Now, you can choose to use DHCP or a specific IP address.



4) **Using DHCP:** If you want to use DHCP, choose **"Obtain an IP address automatically"**, and then click ***OK***. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from WMS-208.

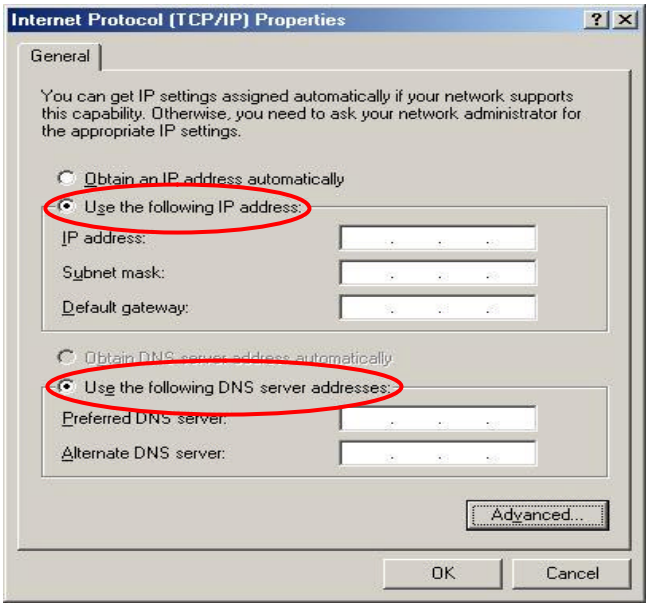

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

5) **Using Specific IP Address:** If you want to use a specific IP address, acquire the following information from the network administrator: the *IP Address*, *Subnet Mask* and *DNS Server address* provided by your ISP and the *Gateway address* of WMS-208.

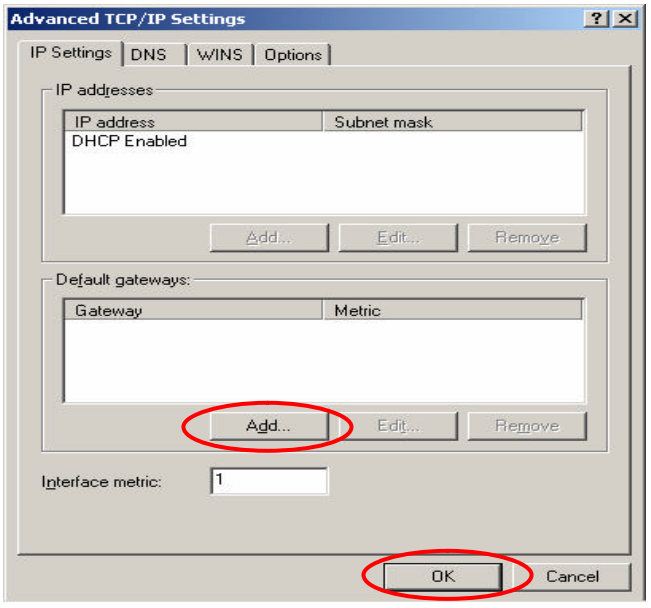
Note: *If your PC has been set up completed, please inform the network administrator before proceeding to the following steps.*

5.1) Choose **"Use the following IP address"** and enter the *IP address*, *Subnet mask*. If the DNS Server field is empty, select **"Using the following DNS server addresses"** and enter the *DNS Server address*. Then, click ***OK***.

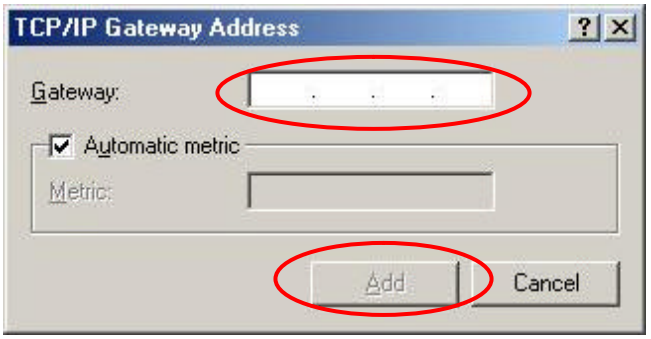
5.2) Click ***Advanced*** to enter the **Advanced TCP/IP Settings** window.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

5.3) Click on the **IP Settings** tab and click ***Add*** below the **"Default gateways"** column and the **TCP/IP Gateway Address** window will appear.

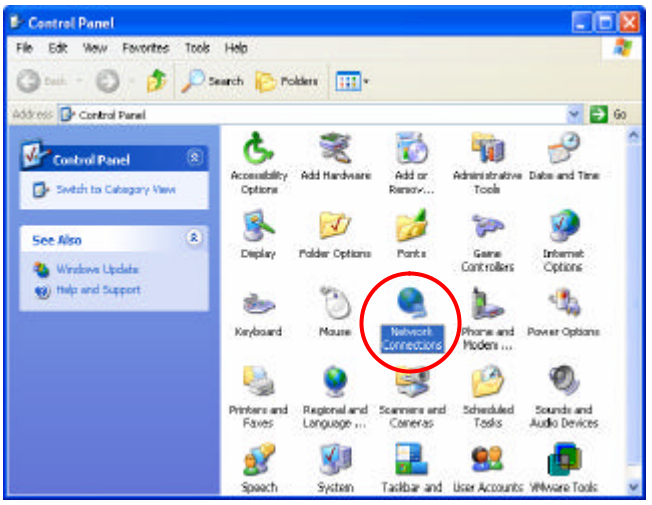


5.4) Enter the gateway address of WMS-208 in the **"Gateway"** field, and then click ***Add***. After back to the **IP Settings** tab, click ***OK*** to complete the configuration.

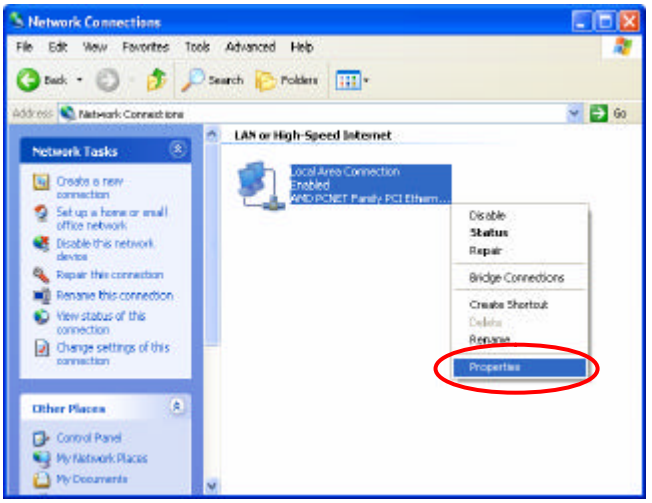


◆ **Check the TCP/IP Setup of Window XP**

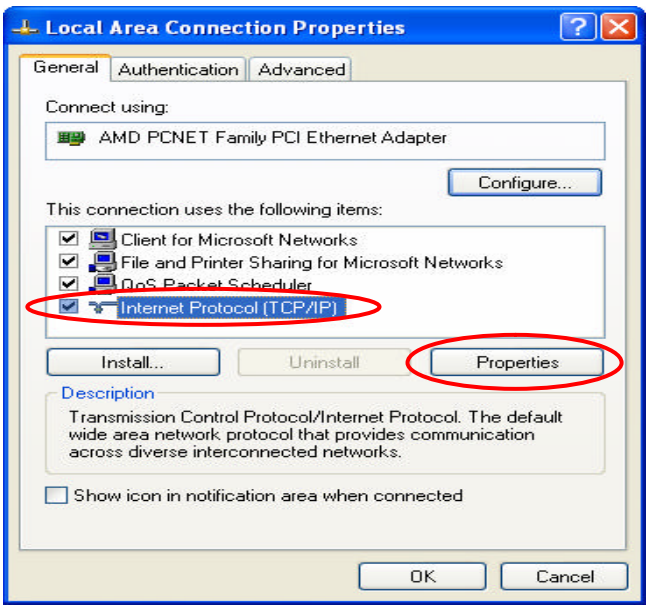
1) Select **Start** >> **Control Panel** >> **Network Connection**.



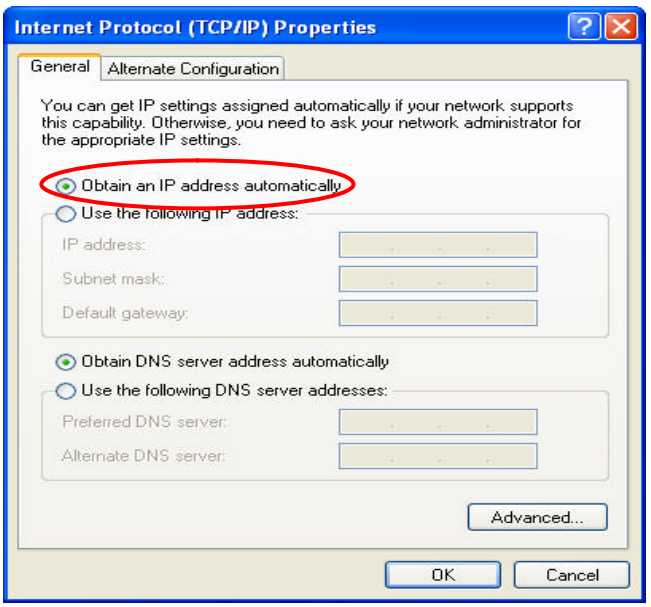
2) Right click on the **Local Area Connection** icon and select **"Properties"**.



3) Click on the **General** tab and choose **"Internet Protocol (TCP/IP)"**, and then click ***Properties***. Now, you can choose to use DHCP or a specific IP address.



4) **Using DHCP:** If you want to use DHCP, choose **"Obtain an IP address automatically"** and click ***OK***. This is also the default setting of Windows. Then, reboot the PC to make sure an IP address is obtained from WMS-208.


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

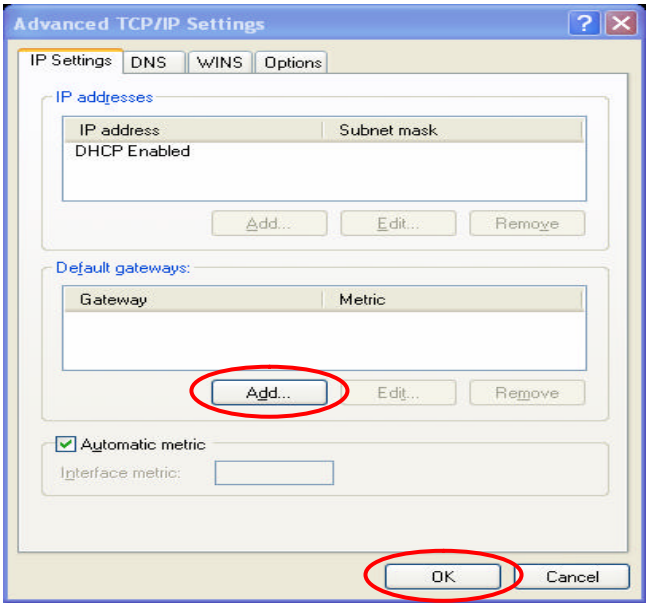
5) **Using Specific IP Address:** If you want to use a specific IP address, acquire the following information from the network administrator: the *IP Address*, *Subnet Mask* and *DNS Server address* provided by your ISP and the *Gateway address* of WMS-208.

Note: *If your PC has been set up completed, please inform the network administrator before proceeding to the following steps.*

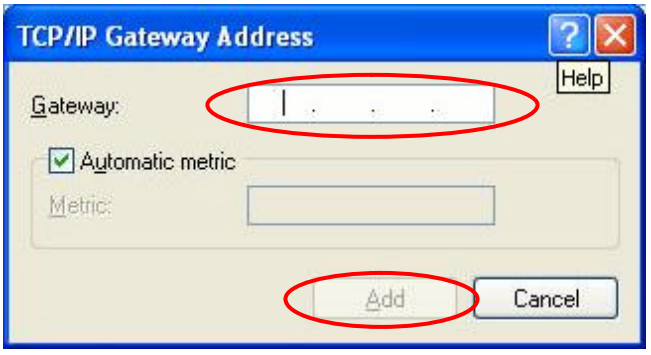
5.1) Choose **"Use the following IP address"** and enter the *IP address*, *Subnet mask*. If the DNS Server field is empty, select **"Using the following DNS server addresses"** and enter the *DNS Server address*. Then, click ***OK***.

5.2) Click ***Advanced*** to enter the **Advanced TCP/IP Settings** window.

5.3) Click on the **IP Settings** tab and click ***Add*** below the **"Default gateways"** column and the **TCP/IP Gateway Address** window will appear.



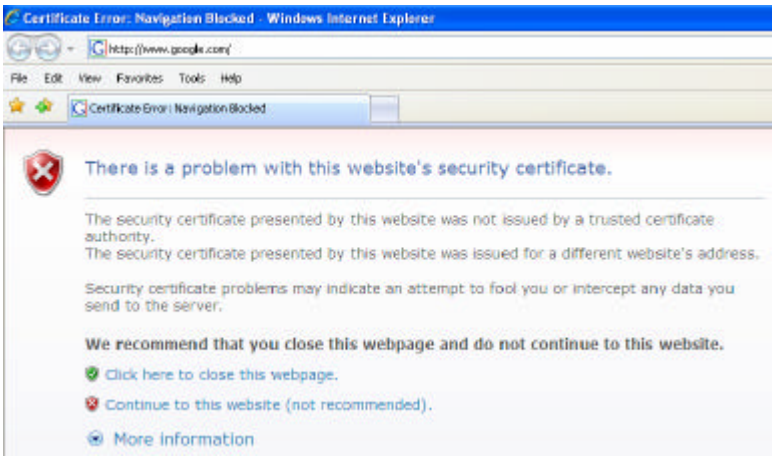
5.4) Enter the gateway address of WMS-208 in the **"Gateway"** field, and then click ***Add***. After back to the **IP Settings** tab, click ***OK*** to finish the configuration.



▪ An Example of User Login

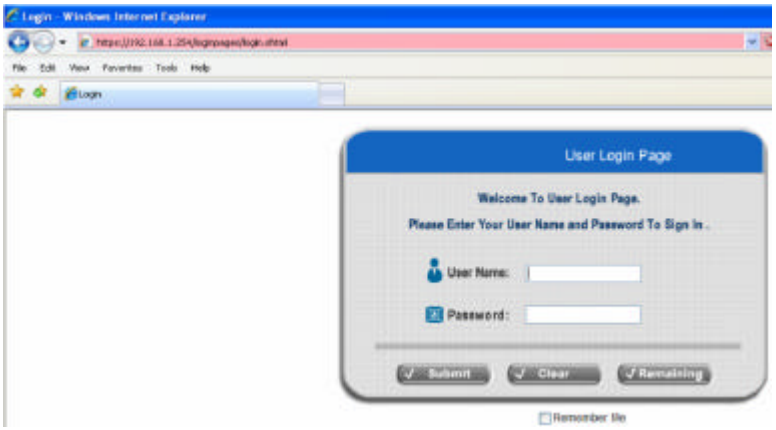
Normally, users will be authenticated before they get network access through WMS-208. This section presents the basic authentication flow for end users. Please make sure that the WMS-208 is configured properly and network related settings are done.

1. Open an Internet browser and try to connect to any website (in this example, we try to connect to www.google.com).
   a For the first time, if the WMS-208 is not using a trusted SSL certificate (for more information, please see *4.2.5 Additional Configuration*), there will be a "Certificate Error", because the browser treats WMS-208 as an illegal website.


Certificate Error: Navigation Blocked - Windows Internet Explorer
There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
The security certificate presented by this website was issued for a different website's address.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

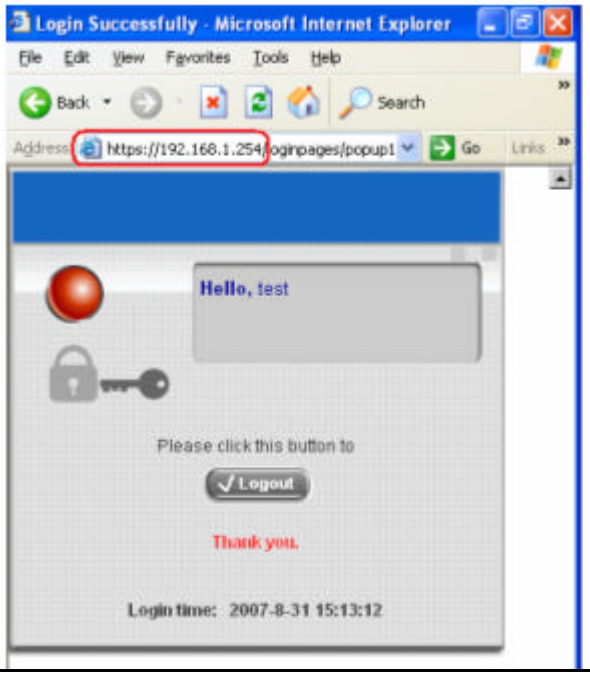
   b Please press "Continue to this website" to continue.

   c The default user login page will appear in the browser.



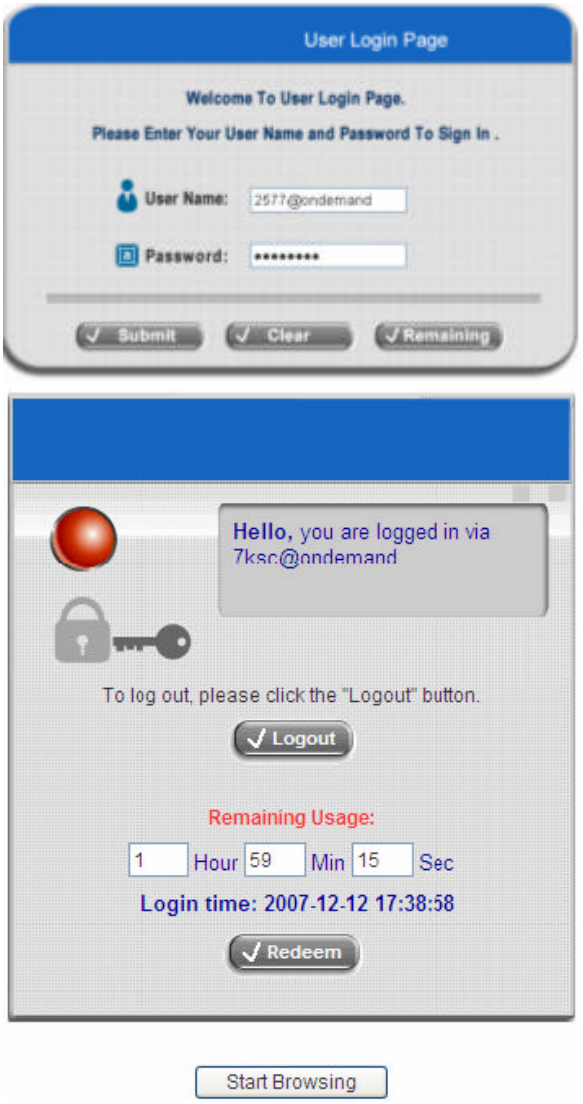
2. Enter the username and password (for example, we use a local user account: **test@local** here) and then click ***Submit*** button. If the ***Remember Me*** check box is checked, the browser will remember this user's name and password so that he/she can just click Submit next time he/she wants to login.
   Check the ***Remember Me*** box to store the username and password on the current computer in order to automatically login to the system at next login. Then, click the ***Submit*** button.
   The ***Remaining*** button on the **User Login Page** is for on-demand users only, where they can check their Remaining Usage time.

3. Successful! The **Login Successful** page appearing means WMS-208 has been installed and configured successfully. Now, you are connected to the network and Internet!



Note: *When On-demand accounts are used (for example, we use* ***7ksc@ondemand*** *here), the system will display more information, as shown below.*

4. **Remaining Usage***:* The remaining quota of this On-demand account that the user can surf the Internet.



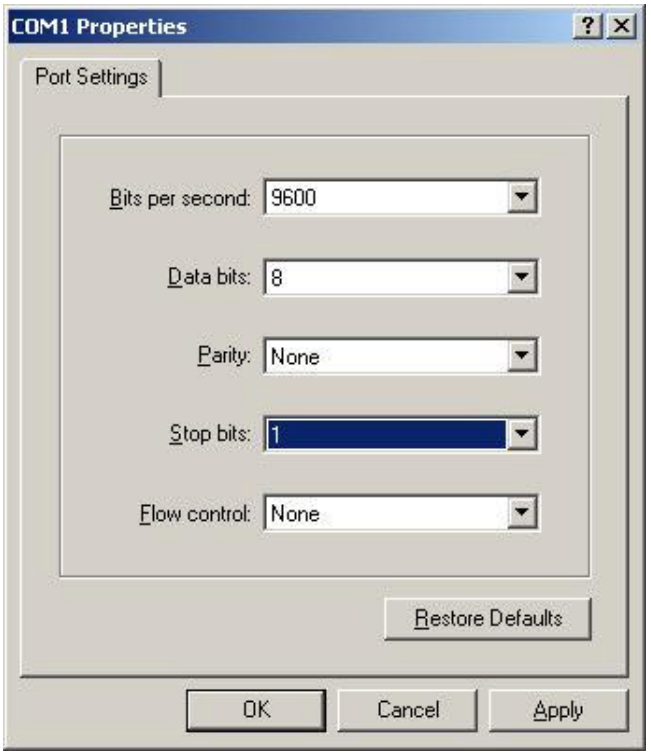
5. **Redeem:** When the remaining quota is insufficient, the user can add up the quota by purchasing an additional account. Please enter the new username and password in the Redeem Page and click ***ENTER*** button to merge the two accounts so that there will be more quota for the original account.

Note: *The maximum session time/data transfer is 24305 days/9,999,999 Mbyte. If the redeem amount exceeds this number, the system will automatically reject the redeem process.*

Appendix G. Console Interface

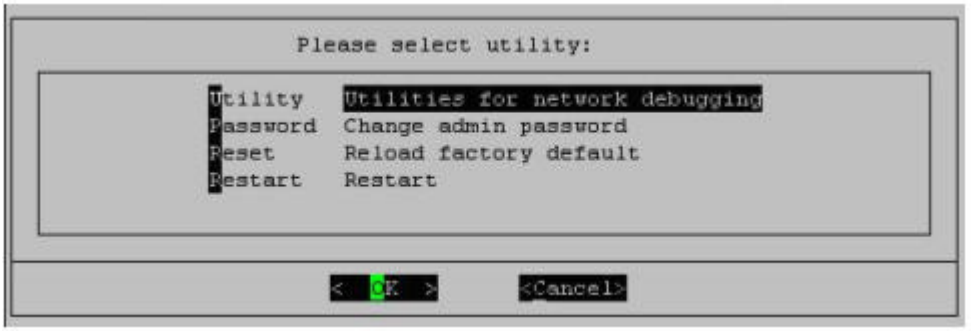
Via this port to enter the console interface for the administrator to handle the problems and situations occurred during operation.

1. In order to connect to the console port of PheeNet WMS-208, a console, modem cable and a terminal simulation program, such as the Hyper Terminal are needed.
2. If a Hyper Terminal is used, please set the parameters as **9600, 8, None, 1, and None**.



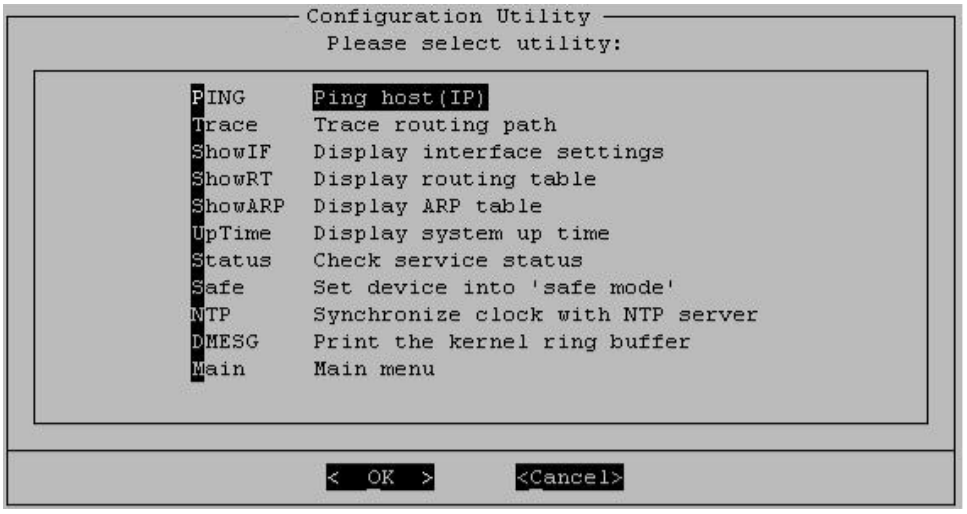
Caution: *the main console is a menu-driven text interface with dialog boxes. Please use arrow keys on the keyboard to browse the menu and press the* ***Enter*** *key to make selection or confirm what you enter.*

3. Once the console port of PheeNet WMS-208 is connected properly, the console main screen will appear automatically. If the screen does not appear in the terminal simulation program automatically, please try to press the arrow keys, so that the terminal simulation program will send some messages to the system, where the welcome screen or main menu should appear. If the welcome screen or main menu of the console still does not pop up, please check the connection of the cables and the settings of the terminal simulation program.



- **Utilities for network debugging**

  The console interface provides several utilities to assist the Administrator to check the system conditions and to debug any problems. The utilities are described as follows:


Configuration Utility
Please select utility:
PING Ping host(IP)
Trace Trace routing path
ShowIF Display interface settings
ShowRT Display routing table
ShowARP Display ARP table
UpTime Display system up time
Status Check service status
Safe Set device into 'safe mode'
NTP Synchronize clock with NTP server
DMESG Print the kernel ring buffer
Main Main menu
< OK >
<Cancel>

  - Ping host (IP): By sending ICMP echo request to a specified host and wait for the response to test the network status.
  - Trace routing path: Trace and inquire the routing path to a specific target.
  - Display interface settings: It displays the information of each network interface setting including the MAC address, IP address, and netmask.
  - Display the routing table: The internal routing table of the system is displayed, which may help to confirm the Static Route settings.
  - Display ARP table: The internal ARP table of the system is displayed.
  - Display system up time: The system live time (time for system being turn on) is displayed.
  - Check service status: Check and display the status of the system.
  - Set device into "safe mode": If the administrator is unable to use Web Management Interface via browser for the system failed inexplicitly. The administrator can choose this utility and set it into safe mode, which enables him to manage this device with browser again.
  - Synchronize clock with NTP server: Immediately synchronize the clock through the NTP protocol and the specified network time server. Since this interface does not support manual setup for its internal clock, therefore we must reset the internal clock through the NTP.
  - Print the kernel ring buffer: It is used to examine or control the kernel ring buffer. The program helps users to print out their boot-up messages instead of copying the messages by hand.
  - Main menu: Go back to the main menu.

- **Change admin password**

  Besides supporting the use of console management interface through the connection of null modem, the system also supports the SSH online connection for the setup. When using a null modem to connect to the system console, we do not need to enter administrator's password to enter the console management interface. But connecting the system by SSH, we have to enter the username and password.

  The username is "admin" and the default password is also "admin", which is the same as for the web management interface. Password can also be changed here. If administrators forget the password and are unable to log in the management interface from the web or the remote end of the SSH, they can still use the null modem to connect the console management interface and set the administrator's password again.

Caution: *Although it does not require a username and password for the connection via the serial port, the same management interface can be accessed via SSH. Therefore, we recommend you to immediately change the PheeNet WMS-208 Admin username and password after logging in the system for the first time.*

- **Reload factory default**

  Choosing this option will reset the system configuration to the factory defaults.

- **Restart PheeNet WMS-208**

  Choosing this option will restart PheeNet WMS-208.

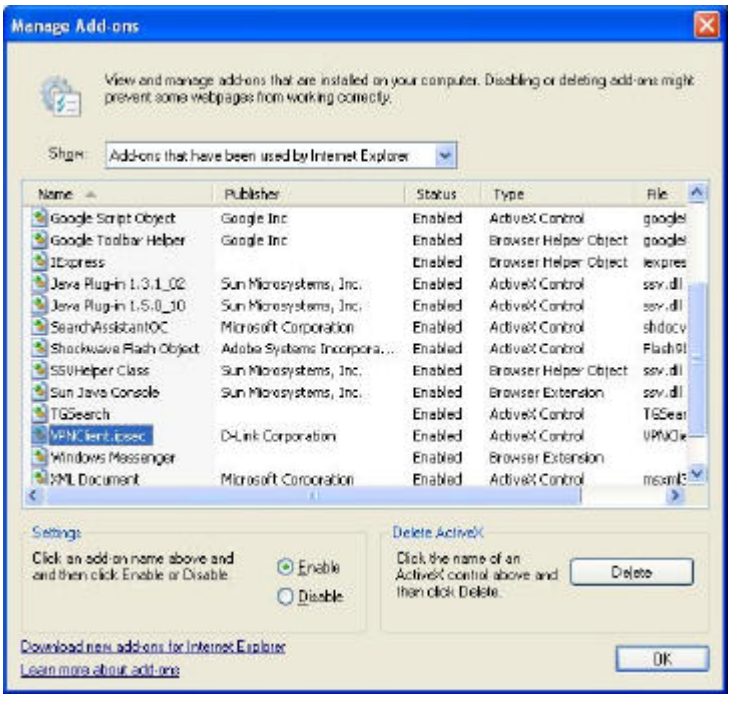
Appendix H. Local VPN

The system is equipped with IPSec VPN feature. To utilize IPSec VPN supported by Microsoft Windows XP SP2 (with patch) and Windows 2000 operating systems, the system implements IPSec VPN tunneling technology between client's windows devices and the system itself regardless of wired or wireless network.

By pushing down ActiveX to the client' s Windows device from the system, no extra client software is required to be installed except ActiveX, in which a so-called "clientless" IPSec VPN setting is then configured automatically. At the end of this setup, a build-in IPSec VPN feature will be enabled and ready to serve once it is launched for setup. The goal of this design is to eliminate the configuration difficulty from IPSec VPN users. At the client side, the IPSec VPN implementation of the system is based on ActiveX and the built-in IPSec VPN client of Windows OS.

1. ActiveX Component

The ActiveX is a software component running inside Internet Explorer. The ActiveX component can be checked by the following windows.



From Windows Internet Explorer, click ***Manage add-ons*** button inside **Programs** page under **Tools** to show the add-ons programs list. You can see **VPNClient.ipsec** is enabled.

During the first-time login to WMS-208, Internet Explorer will ask clients to download an ActiveX component of IPSec VPN. Once this ActiveX component is downloaded, it will run in parallel with the "Login Success Page" after the page being brought up successfully. The ActiveX component helps set up individual IPSec VPN tunnels between clients and WMS-208 and check the validity of IPSec VPN tunnels between them. If the connection is down, the ActiveX component will detect the broken link and decompose the IPSec tunnel. Once the IPSec VPN tunnel was built, all sent packets will be encrypted. Without connecting to the original IPSec VPN tunnel, a client has no alternative way to gain network connection beyond this. IPSec VPN feature supported by WMS-208 directly solves possible data security leak problem between clients and the system via either wireless or wired connections without extra hardware or client software installed.

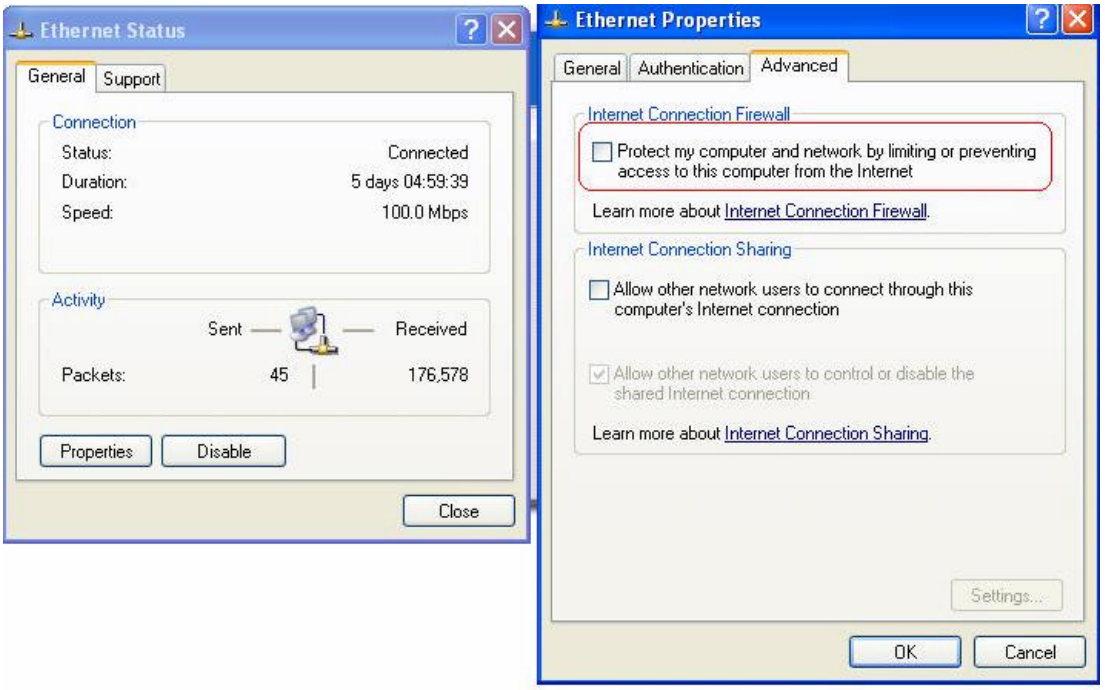
2. Limitations

The limitation on the client side due to ActiveX and Windows OS includes:

- ***a*** Internet Connection Firewall of Windows XP or Windows XP SP1 is not compatible with IPSec protocol. It shall be turned off to allow IPSec packets to pass through.
- ***b*** Without patch, ICMP (Ping) and PORT command of FTP can not work in Windows XP SP2.
- ***c*** The forced termination (through CTRL+ALT+DEL, Task Manager) of the Internet Explorer will stop the running of ActiveX. It causes that IPSec tunnel cannot be cleared properly at client device. A reboot of client device is needed to clear the IPSec tunnel.
- ***d*** The crash of Windows Internet Explorer may cause the same result.

3. Internet Connection Firewall

In Windows XP and Windows XP SP1, the Internet Connection Firewall is not compatible with IPSec. Internet Connection Firewall will drop packets from tunneling of IPSec VPN.



Suggestion: *Please* ***TURN OFF*** *Internet Connection Firewall feature or upgrade the Windows OS into Windows XP SP2.*

4. ICMP and Active Mode FTP

On Windows XP SP2 that is without patch KB889527, ICMP packets will be dropped from IPSec tunnel. This issue can be fixed by upgrading patch KB889527. Before enabling IPSec VPN function on client device, please access the patch from Microsoft' s web at: http://support.microsoft.com/default.aspx?scid=kb;en-us;889527.
This patch also fixes issues of supporting active mode FTP inside IPSec VPN tunnel of Windows XP SP2.

Suggestion: *Please UPDATE client's Windows XP SP2 with patch KB889527.*

5. The Termination of ActiveX

The ActiveX component for IPSec VPN is running parallel with the "Login Success" web page. Unless user decides to close the session and to disconnect with the system, the following conditions or behaviors of user' s browser can be avoided in order to maintain the built IPSec VPN tunnel always alive.
Reasons why Internet Explorer may cause ActiveX to stop unexpectedly are as follows:

a. The crash of Internet Explorer on running ActiveX

Suggestion: *Please reboot client's computer once Windows service is resumed. Go through the login process again.*

b. **Terminate the Internet Explorer Task from Windows Task Manager**

Suggestion: *Do not terminate this VPN task of Internet Explorer.*

c **There are some cases of Windows messages by which the system will hint current user to:**

(1) Close the Windows Internet Explorer.

(2) Click ***logout*** on login success page.

(3) Click ***back*** or ***refresh*** of the same Internet Explorer.

(4) Enter new URL in the same Internet Explorer.

(5) Open a URL from the other application (e.g. email of Outlook) that occupies this existing Internet Explorer.

All these will cause the termination of IPSec VPN tunneling if the user chooses to click "Yes". The user has to log in again to regain the network access.

Suggestion: *Click "Cancel" if you do not intend to stop the IPSec VPN connection yet.*

6. Non-supported OS and Browser

Currently, Windows Internet Explorer is the only browser supported by the system. Windows XP and Windows 2000 are the only two supported OS along with this release.

7. FAQ

a. How to clean IPSec client?

ANS:

Open a command prompt window and type the commands as follows.

C:\> **cd %windir%\system32**

C:\> **Clean_IPSEC.bat**

Or

C:\> **cd %windir%\system32**

C:\> **ipsec2k.exe stop**

b. How to remove ActiveX component in client's computer?

ANS:

(1) Uninstall and delete ActiveX component

(2) Close all Internet Explorer windows

(3) Open a command prompt window and type the commands as follows

C:\> **cd %windir%\system32**

C:\> **regsvr32 /u VPNClient_1_5.ocx**

C:\> **del VPNClient_1_5.ocx**

c. What can I do if unable establish IPSec connection for Windows XP SP1?

ANS:

Disable Windows XP firewall

Appendix I. Customizable Pages

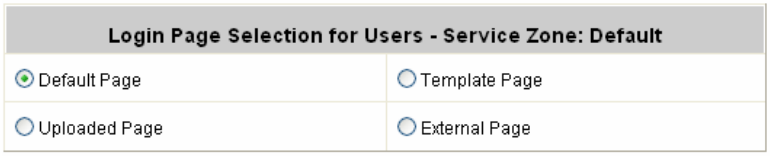
There are five users' login and logout pages for each service zone that can be customized by administrators.
Go to System Configuration >> Service Zone >> Service Zone Settings Configure >> Custom Pages.
Click the button of ***Configure***, the **Login (Logout)** page will appear, including **Login page**, **Logout Page**, **Login Success Page**, **Login Success Page for On-demand User** and **Logout Success Page**.
Click the radio button of page selections to have further configuration.

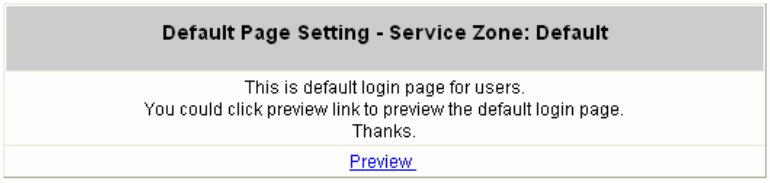
1 *Custom Pages >>* ***Login Page***

The administrator can use the default login page or get the customized login page by setting the template page, uploading the page or downloading from the specific website. After finishing the setting, click ***Preview*** to see the login page.

- *Custom Pages >> Login Page >>* ***Default Page***

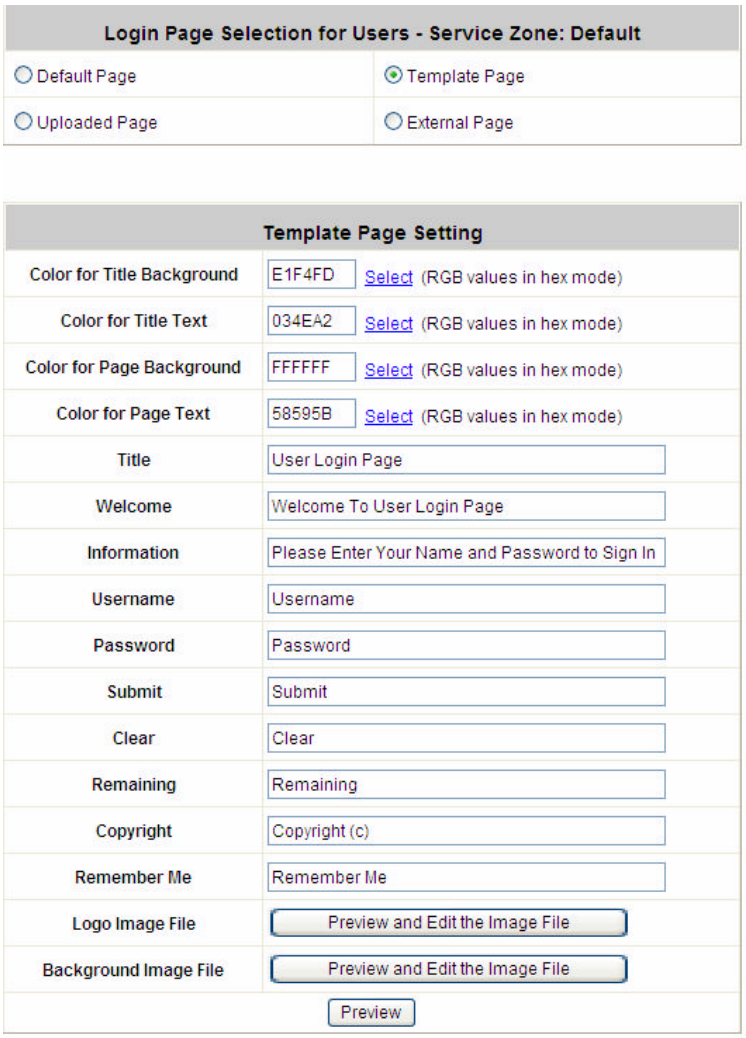
  Choose Default Page to use the default login page.




Default Page Setting - Service Zone: Default
This is default login page for users.
You could click preview link to preview the default login page.
Thanks.
Preview

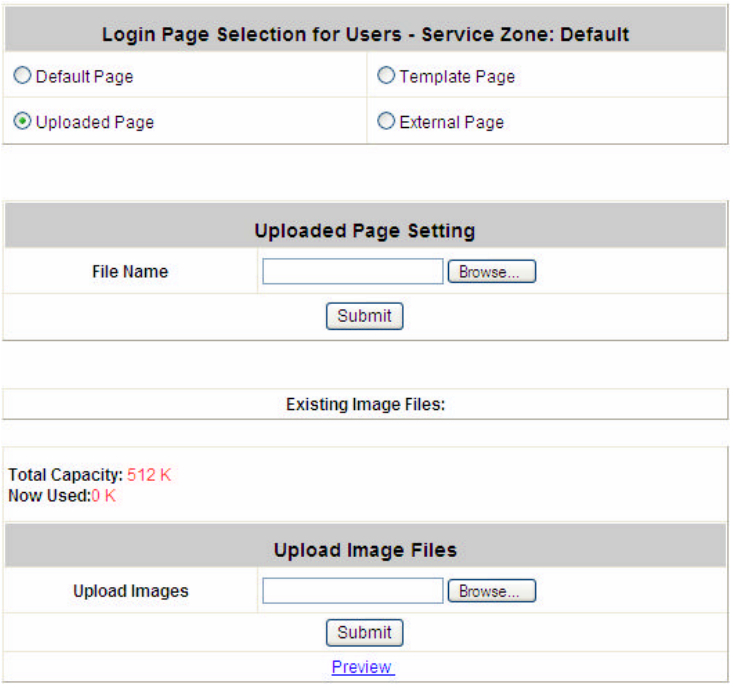
- *Custom Pages >> Login Page >>* ***Template Page***

  Choose Template Page to make a customized login page. Click Select to pick up a color and then fill in all of the blanks. You can also upload a background image file for your template. Click ***Preview*** to see the result first.



- *Custom Pages >> Login Page >>* ***Uploaded Page***

  Choose Uploaded Page and upload a login page.



The user-defined login page must include the following HTML codes to provide the necessary fields for user name and password.

```
<form action="userlogin.shtml" method="post" name="Enter">
<input type="text" name="myusername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value="Enter">
<input type="reset" name="clear" value="Clear">
</form>
```

And if the user-defined login page includes an image file, the image file path in the HTML code must be the image file to be uploaded.

Remote VPN : <img src=images/xx.jpg”>
Default Service Zone: <img src=images0/xx.jpg”>
Service Zone 1 : <img src=images1/xx.jpg”>
Service Zone 2 : <img src=images2/xx.jpg”>
Service Zone 3 : <img src=images3/xx.jpg”>
Service Zone 4 : <img src=images4/xx.jpg”>

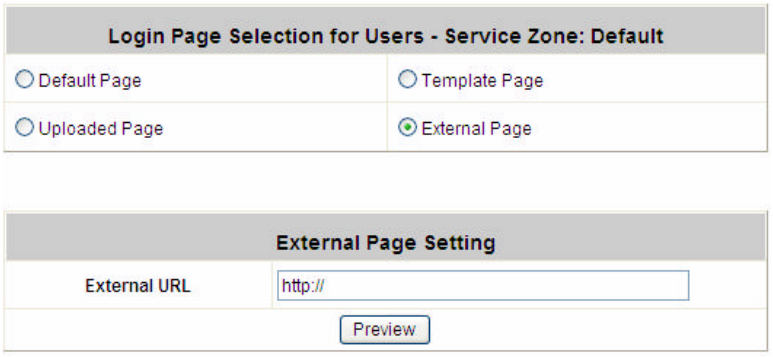
Click the ***Browse*** button to select the file to upload. Then click ***Submit*** to complete the upload process.

Next, enter or browse the filename of the images to upload in the **Upload Images** field on the **Upload Images Files** page and then click ***Submit***. The system will show the used space and the maximum size of the image file of 512K. If the administrator wishes to restore the factory default of the login page, click the ***Use Default Page*** button to restore it to default.

After the image file is uploaded, the file name will show on the **“Existing Image Files”** field. Check the file and click ***Delete*** to delete the file.

After the upload process is completed and applied, the new login page can be previewed by clicking ***Preview*** button at the button.

- *Custom Pages >> Login Pages >>* ***External Page***



Choose the ***External Page*** selection and get the login page from the specific website. In the External Page Setting, enter the URL of the external login page and then click ***Apply***.

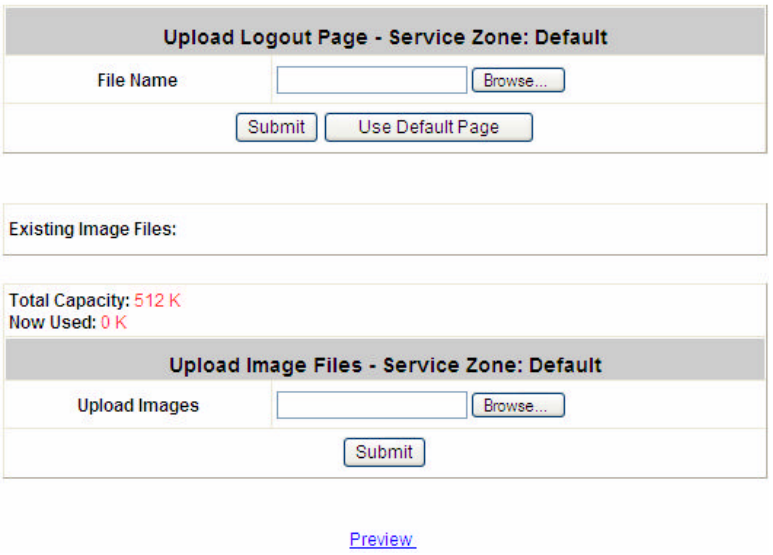
After applying the setting, the new login page can be previewed by clicking ***Preview*** button at the bottom of this page.

The user-defined logout page must include the following HTML codes to provide the necessary fields for username and password.

```
<form action="userlogin.shtml" method="post" name="Enter">
<input type="text" name="myusername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value="Enter">
<input type="reset" name="clear" value="Clear">
</form>
```

2 *Custom Pages >>* ***Logout Page***

The administrator can apply their own logout page in the menu. As the process is similar to that of the Login Page, please refer to the "Login Page >> Uploaded Page" instructions for more details.



Note*: The different part is the HTML code of the user-defined logout interface must include the following HTML code that the user can enter the username and password. After the upload is completed, the customized logout page can be previewed by clicking* ***Preview*** *at the bottom of this page. If restore to factory default setting is needed for the logout interface, click the "****Use Default Page"*** *button.*

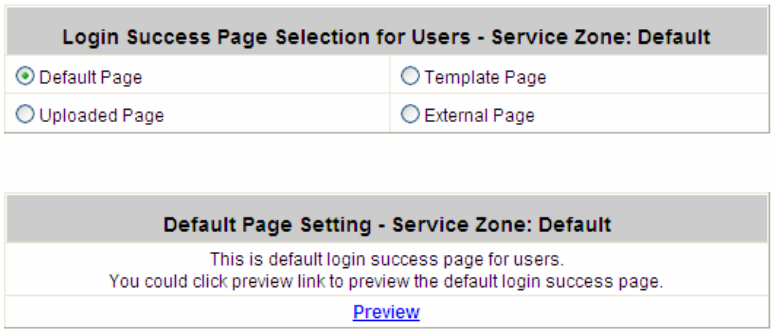
```
<form action="userlogout.shtml" method="post" name="Enter">
<input type="text" name="myusername">
<input type="password" name="mypassword">
<input type="submit" name="submit" value="Logout">
<input type="reset" name="clear" value="Clear">
</form>
```

3 *Custom Pages >>* ***Login Success Page***

The users can apply their own Login Success page in the menu. As the process is similar to that of the Login Page, please refer to the "Login Page" instructions for more details.

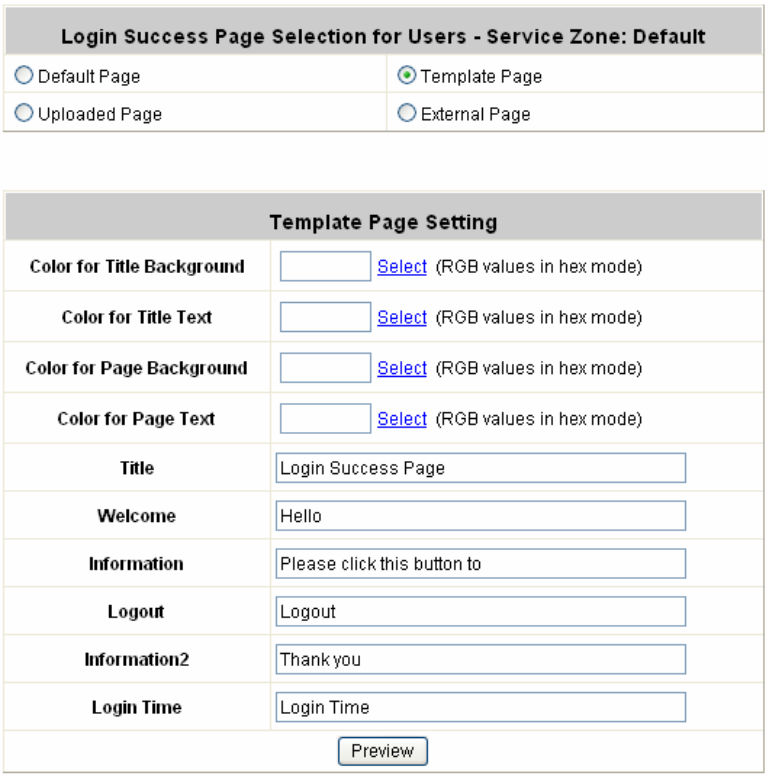
- *Custom Pages >> Login Success Page >>* ***Default Page***

  Choose Default Page to use the default login success page.


Login Success Page Selection for Users - Service Zone: Default
Default Page
Template Page
Uploaded Page
External Page
Default Page Setting - Service Zone: Default
This is default login success page for users.
You could click preview link to preview the default login success page.
Preview

- *Custom Pages >> Login Success Page >>* ***Template Page***

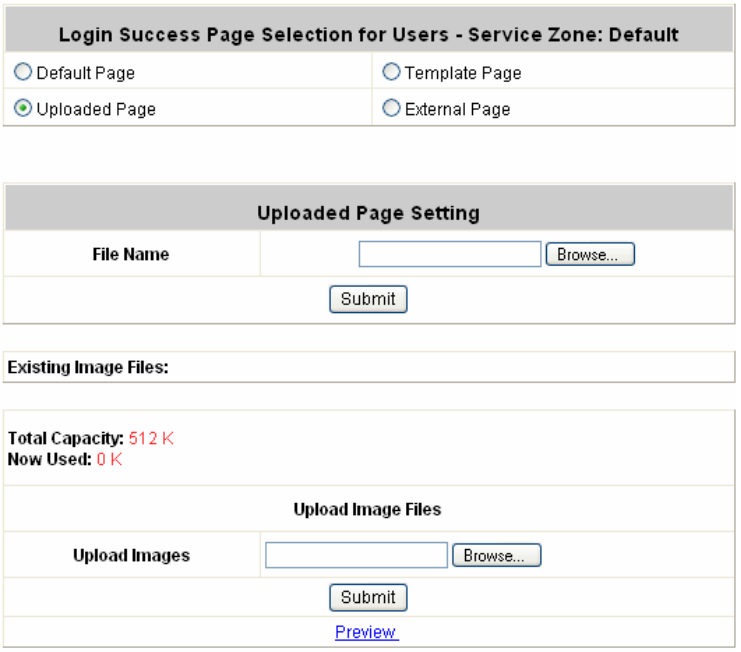
  Choose Template Page to make a customized login success page. Click Select to pick up a color and then fill in all of the blanks. Click Preview to see the result first.



- *Custom Pages >> Login Success Page >>* ***Uploaded Page***

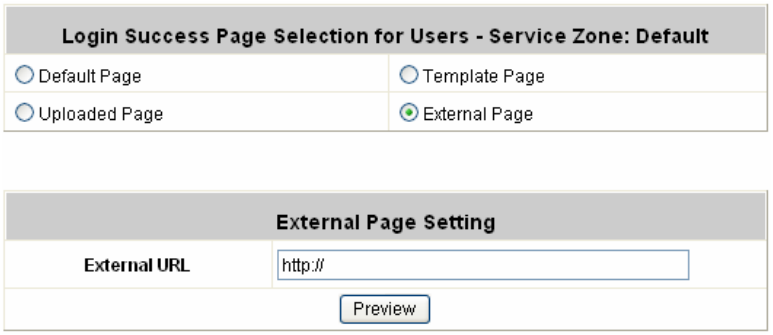
  Choose Uploaded Page and get the login success page to upload. Click the Browse button to select the file for the login success page upload. Then click Submit to complete the upload process.

  After the upload process is completed and applied, the new login success page can be previewed by clicking Preview button at the bottom.



- *Custom Pages >> Login Success Page >>* ***External Page***

  Choose the External Page selection and get the login success page from the specific website. In the External Page Setting, enter URL of the external login page and then click Apply. After applying the setting, the new login success page can be previewed by clicking ***Preview*** button at the bottom of this page

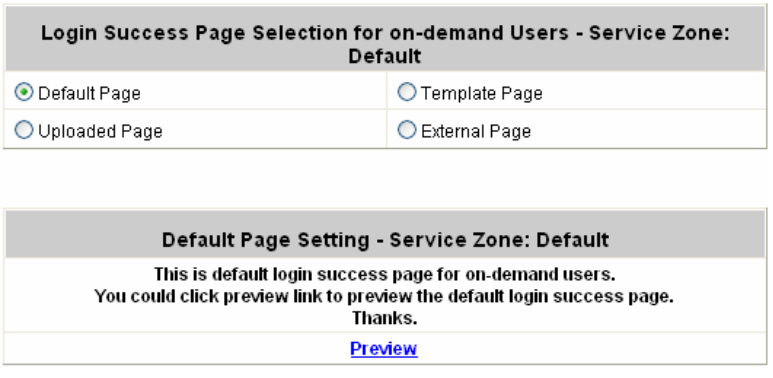


4 *Custom Pages >>* ***Login Success Page for On-demand User***

The users can apply their own Login Success page for on-demand Users in the menu. As the process is similar to that of the Login Page, please refer to the "Login Page" instructions for more details.

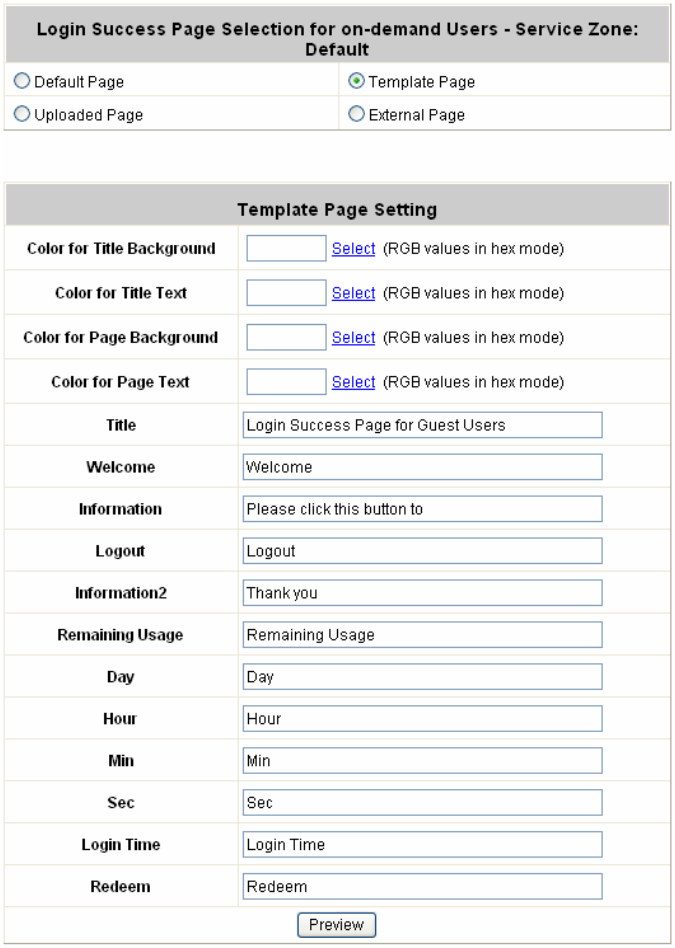
- *Custom Pages >> Login Success Page for On-demand Users >>* ***Default Page***

  Choose Default Page to use the default login success page for on-demand account


Login Success Page Selection for on-demand Users - Service Zone: Default
Default Page
Template Page
Uploaded Page
External Page
Default Page Setting - Service Zone: Default
This is default login success page for on-demand users.
You could click preview link to preview the default login success page.
Thanks.
Preview

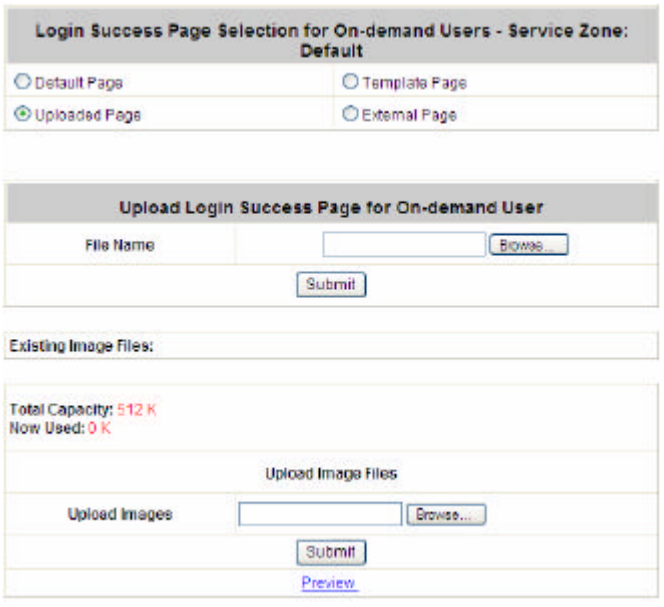
- *Custom Pages>> Login Success Page for On-demand Users>>* ***Template Page***

  Choose Template to make a customized login success for on-demand account. Click *Select* to pick up a color and then fill in all of the blanks. Click ***Preview*** to see the result.



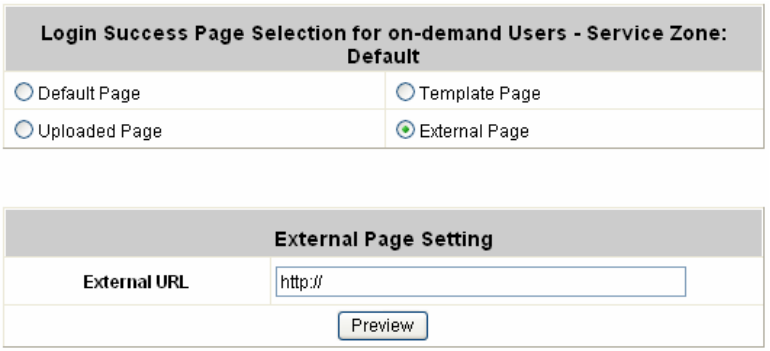
- *Custom Pages>> Login Success Pages for On-demand Users>>* ***Uploaded Page***

  Choose Uploaded Page and get the login success page for on-demand users by uploading. Click the ***Browse*** button to select the file for the login success page for Instant upload. Then click ***Submit*** to complete the upload process.



- *Custom Pages >> Login Success Pages for On-demand Users >>* ***External Page***

  Choose the External Page selection and get the login success page from the specific website. In the External Page Setting, enter URL of the external login page and then click Apply. After applying the setting, the new login success page can be previewed by clicking ***Preview*** button at the bottom of this page.

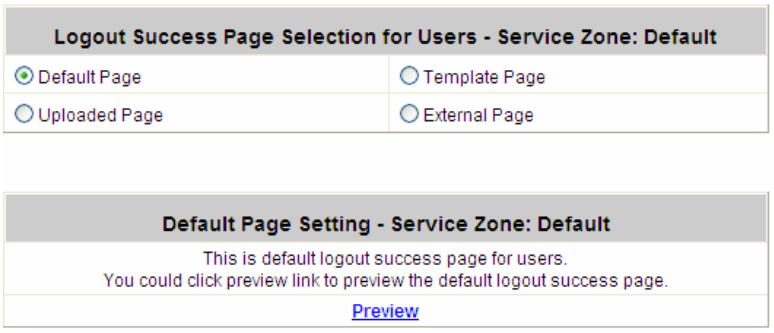


5 *Custom Pages >>* ***Logout Success Page***

The administrator can apply their own Logout Success page for Users in the menu. As the process is similar to that of the Login Page, please refer to the "Login Page" instructions for more details.

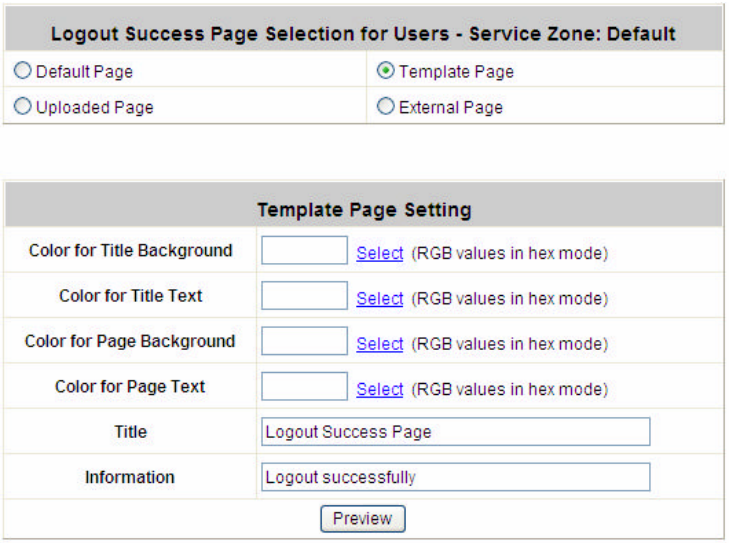
- *Custom Pages >> Logout Success Page >>* ***Default Page***

  Choose ***Default Page*** to use the default logout success page.


Logout Success Page Selection for Users - Service Zone: Default
Default Page
Template Page
Uploaded Page
External Page
Default Page Setting - Service Zone: Default
This is default logout success page for users.
You could click preview link to preview the default logout success page.
Preview

- *Custom Pages >> Logout Success Page >>****Template Page***

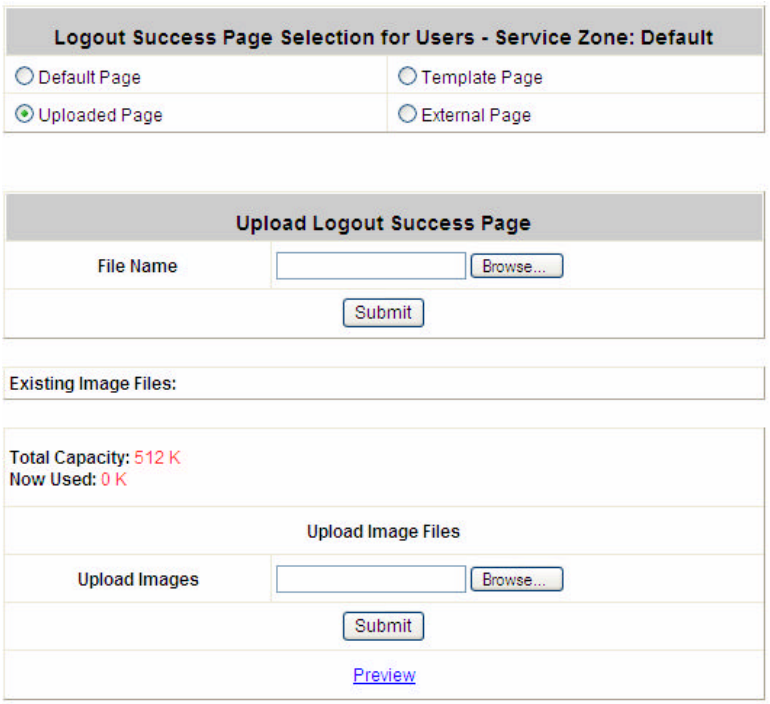
  Choose Template Page to make a customized logout success page. Click ***Select*** to pick up a color and then fill in all of the blanks. Click ***Preview*** to see the result first.



- *Custom Pages >> Logout Success Page >>* ***Uploaded Page***

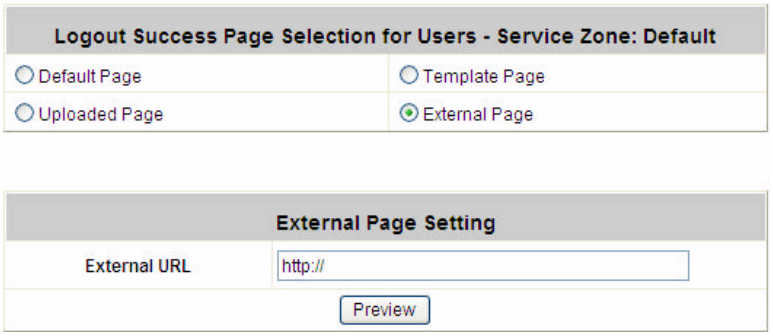
  Choose Uploaded Page and get the logout success page to upload. Click the ***Browse*** button to select the file for the logout success page upload. Then click ***Submit*** to complete the upload process.

  After the upload process is completed and applied, the new logout success page can be previewed by clicking ***Preview*** button at the bottom.



- *Custom Pages >>Logout Success Page >>* ***External Page***

  Choose the External Page selection and get the logout success page from the specific website. Enter the website address in the External Page Setting field and then click Apply. After applying the setting, the new logout success page can be previewed by clicking ***Preview*** button at the bottom of this page.



P/N: 31220080522